日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００１年　５月３１日

出 願 番 号
Application Number: 特願２００１－１６５５８０

パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is ＪＰ２００１－１６５５８０

出 願 人
Applicant(s): トレンドマイクロ株式会社

２００９年１０月１５日

特許庁長官
Commissioner,
Japan Patent Office 細野哲弘

【書類名】特許願

【整理番号】TM-01

【提出日】平成13年 5月31日

【あて先】特許庁長官　殿

【国際特許分類】

G06F 13/00

H04L　9/00

H04L 12/28

H04L 12/46

H04L 12/66

【発明の名称】データ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体

【請求項の数】 28

【発明者】

【住所又は居所】アール．オー．シー，台湾，台北，チュン　フォア，エス．アールディー．エスイーシー．２，３１９，９階　トレンドマイクロ　インコーポレイテッド

【氏名】リー，フランク

【特許出願人】

【識別番号】397011166

【氏名又は名称】トレンドマイクロ株式会社

【代理人】

【識別番号】100098084

【弁理士】

【氏名又は名称】川▲崎▼　研二

【選任した代理人】

【識別番号】100111763

【弁理士】

【氏名又は名称】松本　隆

【手数料の表示】

【予納台帳番号】038265

【納付金額】21,000

【提出物件の目録】

【物件名】明細書　1

【物件名】図面　1

【物件名】要約書　1

【プルーフの要否】要

【書類名】　　明細書

【発明の名称】　データ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体

【特許請求の範囲】

【請求項１】　データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置が、受信したデータを予め定められたサーバに転送するステップと、

前記サーバが、前記データ中継装置から転送されてくるデータを受信し、当該データの宛先へ送信するステップと、

前記サーバが、前記送信したデータに応答して前記宛先から送信されてくる応答データを受信するステップと、

前記サーバが、前記宛先から受信した応答データに対してセキュリティチェックを行うステップと、

前記サーバが、前記セキュリティチェックを行った後の応答データを前記データ中継装置を介して前記情報通信装置に送信するステップと

を備えることを特徴とするデータ通信方法。

【請求項２】　データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置が、受信したデータを予め定められたサーバに転送するステップと、

前記サーバが、前記データ中継装置から転送されてくるデータを受信するステップと、

前記サーバが、前記受信したデータに対してセキュリティチェックを行うステップと、

前記サーバが前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するステップと

を備えることを特徴とするデータ通信方法。

【請求項３】　請求項１又は２に記載のデータ通信方法において、

前記情報通信装置は、プロバイダが提供するインターネット接続サービスを受けることにより、インターネットを介してデータを送受信する装置であり、

前記プロバイダの通信装置が、前記情報通信装置のユーザが前記サーバによって行われるセキュリティチェックを受けるための契約情報を当該情報通信装置から受信するステップと、

前記プロバイダの通信装置が、前記受信した契約情報を前記サーバに転送するステップと、

前記サーバが、前記サーバから転送されてくる契約情報を受信し、記憶するステップと

を備え、

前記セキュリティチェックを行うステップにおいて、前記サーバは前記記憶している契約情報に基づいて前記セキュリティチェックを行う

ことを特徴とするデータ通信方法。

【請求項４】　請求項３に記載のデータ通信方法において、

前記プロバイダの通信装置が、前記受信した契約情報に基づいて、前記データ中継装置においてデータ転送の要否を判断するための情報を当該データ中継装置に転送するステップと、

前記データ中継装置が、前記プロバイダの通信装置から転送されてくる情報を受信し、記憶するステップと

を備え、

前記データ中継装置が転送するステップにおいて、前記データ中継装置は前記記憶している情報に基づいて前記転送の要否を判断して前記転送を行う

ことを特徴とするデータ通信方法。

【請求項５】　請求項１又は２に記載のデータ通信方法において、

前記情報通信装置は、プロバイダが提供するインターネット接続サービスを受けることにより、インターネットを介してデータを送受信する装置であり、

前記プロバイダの通信装置が、前記サーバによって行われるセキュリティチェックの内容に応じて、前記情報通信装置のユーザに課金するための処理を行うステップを備えることを特徴とするデータ通信方法。

【請求項６】　データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置と、データに対してセキュリティチェックを行うサーバと

からなるデータ通信システムであって、

前記データ中継装置が、

受信したデータを前記サーバに転送する転送手段を備え、

前記サーバが、

前記データ中継装置から転送されてくるデータを受信するデータ受信手段と、

前記受信したデータを当該データの宛先へ送信するデータ送信手段と、

前記送信したデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信手段と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後の応答データを前記データ中継装置を介して前記情報通信装置に送信する応答データ送信手段と

を備えることを特徴とするデータ通信システム。

【請求項７】　データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置と、データに対してセキュリティチェックを行うサーバとからなるデータ通信システムであって、

前記データ中継装置が、

受信したデータを前記サーバに転送する転送手段を備え、

前記サーバが、

前記データ中継装置から転送されてくるデータを受信するデータ受信手段と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信手段と

を備えることを特徴とするデータ通信システム。

【請求項８】　データの送受信を行って当該データの伝送を中継する通信手段と、

前記通信手段によって受信された受信データを、転送されてきたデータに対してセキュリティチェックを行うサーバへ前記通信手段を用いて転送する転送手段

と

を備えることを特徴とするデータ中継装置。

【請求項９】　請求項８に記載のデータ中継装置において、

前記転送手段によって前記受信データを前記サーバへ転送する必要があるか否かを判断する判断手段を備え、

前記転送手段は、前記判断手段によって転送要と判断された場合に前記受信データを前記サーバへ転送することを特徴とするデータ中継装置。

【請求項１０】　請求項９に記載のデータ中継装置において、

前記判断手段は、前記受信データの送信元が前記サーバでない場合に転送要と判断することを特徴とするデータ中継装置。

【請求項１１】　請求項１０に記載のデータ中継装置において、

外部の通信装置から送信されてくる前記サーバの通信アドレスを受信するアドレス受信手段と、

前記受信した通信アドレスを記憶するアドレス記憶手段と

を備え、

前記判断手段は、前記受信データに含まれている当該受信データの送信元の通信アドレスと、前記アドレス記憶手段に記憶されている通信アドレスとに基づいて前記転送の要否を判断することを特徴とするデータ中継装置。

【請求項１２】　請求項９に記載のデータ中継装置において、

前記判断手段は、

前記受信データが従うプロトコルに基づいて転送の要否を判断するための要否判断情報を記憶する要否判断情報記憶手段と、

前記受信データに含まれているプロトコル識別情報と、前記要否判断情報記憶手段に記憶されている要否判断情報とに基づいて前記転送の要否を決定する決定手段と

を備えることを特徴とするデータ中継装置。

【請求項１３】　請求項１２に記載のデータ中継装置において、

外部の通信装置から送信されてくる前記要否判断情報を受信する要否判断情報受信手段を備え、

前記要否判断情報記憶手段は、前記受信した要否判断情報を記憶することを特徴とするデータ中継装置。

【請求項１４】　データの送受信を行って当該データの伝送を中継する通信手段と、

自装置に固定的に割り当てられ、自装置を他のデータ中継装置と識別するための装置識別情報を記憶する記憶手段と、

前記通信手段によって受信された受信データに対して前記記憶手段に記憶されている装置識別情報を付加し、当該装置識別情報が付加された受信データを予め定められた転送先へ前記通信手段を用いて転送する転送手段と

を備えることを特徴とするデータ中継装置。

【請求項１５】　請求項１４に記載のデータ中継装置において、

前記装置識別情報は前記データ中継装置のシリアルナンバーであり、

前記転送手段は、前記転送先へ転送する受信データにおけるトランスポート層プロトコルのペイロードに前記シリアルナンバーを書き込んで当該受信データを転送することを特徴とするデータ中継装置。

【請求項１６】　請求項８～１５のいずれか１に記載のデータ中継装置において、

前記データ中継装置は、ネットワーク層プロトコルに従ってルーティングを行うルータであることを特徴とするデータ中継装置。

【請求項１７】　データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信手段と、

前記受信したデータを当該データの宛先へ送信するデータ送信手段と、

前記データ送信手段によって送信されたデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信手段と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後の応答データを前記情報通信装置に送信する応答データ送信手段と

を備えることを特徴とするサーバ。

【請求項１８】　請求項１７に記載のサーバにおいて、

前記セキュリティチェックを行う対象となる応答データは、前記情報通信装置宛のコンテンツであることを特徴とするサーバ。

【請求項１９】　請求項１７に記載のサーバにおいて、

前記セキュリティチェックを行う対象となる応答データは、前記情報通信装置宛の電子メールであることを特徴とするサーバ。

【請求項２０】　データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信手段と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信手段と

を備えることを特徴とするサーバ。

【請求項２１】　請求項２０に記載のサーバにおいて、

前記セキュリティチェックを行う対象となるデータは、前記情報通信装置が送信した電子メールであることを特徴とするサーバ。

【請求項２２】　請求項１７又は２０に記載のサーバにおいて、

正当な前記データ中継装置に割り当てられた識別情報を記憶する記憶手段を参照し、当該記憶手段に記憶されている識別情報と、前記データに付加されて転送されてくる当該データの転送元のデータ中継装置の識別情報とを照合することにより、前記転送元のデータ中継装置の正当性を確認する認証手段を備えることを特徴とするサーバ。

【請求項２３】　請求項２２に記載のサーバにおいて、

前記識別情報は前記データ中継装置のシリアルナンバーであり、

前記データに付加されるシリアルナンバーは、当該データにおけるトランスポート層プロトコルのペイロードに書き込まれており、

前記認証手段は、前記データにおけるトランスポート層プロトコルのペイロードに書き込まれたシリアルナンバーを読み出して前記正当性の確認を行うことを特徴とするサーバ。

【請求項２４】　コンピュータに、

データの送受信を行って当該データの伝送を中継する通信機能と、

前記通信機能によって受信された受信データを、転送されてきたデータに対してセキュリティチェックを行うサーバへ前記通信機能を用いて転送する転送機能と

を実行させるためのプログラム。

【請求項２５】　コンピュータに、

データの送受信を行って当該データの伝送を中継する通信機能と、

自装置に固定的に割り当てられ、自装置を他のデータ中継装置と識別するための装置識別情報を記憶する記憶機能と、

前記通信機能によって受信された受信データに対して前記記憶機能によって記憶されている装置識別情報を付加し、当該装置識別情報が付加された受信データを予め定められた転送先へ前記通信機能を用いて転送する転送機能と

を実行させるためのプログラム。

【請求項２６】　コンピュータに、

データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信機能と、

前記受信したデータを当該データの宛先へ送信するデータ送信機能と、

前記データ送信機能によって送信されたデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信機能と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック機能と、

前記セキュリティチェックを行った後の応答データを前記情報通信装置に送信する応答データ送信機能と

を実行させるためのプログラム。

【請求項２７】　コンピュータに、

データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信機能と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェッ

ク機能と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信機能と

を実行させるためのプログラム。

【請求項２８】　請求項２４～２７のいずれか１に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、インターネット等のコンピュータネットワークにおいて、様々な不正行為による被害を防止するためのデータ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体に関する。

【０００２】

【従来の技術】

インターネットはオープンなネットワーク環境であるがゆえに、世界規模で急速に普及してきた。しかし、その一方で、いわゆるコンピュータウィルスやジャンクメール等の不正行為による被害が数多く発生している。

そこで、これらの問題に対する対抗策が従来から各種提案されている。例えばコンピュータウィルスに対してはワクチンソフトと呼ばれる対抗策が採られている。このワクチンソフトは、コンピュータの外部から進入してきたコンピュータウィルスを検出してこれを駆除するためのコンピュータプログラムであり、ユーザのパソコンにインストールして利用される。

【０００３】

【発明が解決しようとする課題】

コンピュータウィルスの検出技術の代表的なものとして、例えばパターンマッチング方式がある。これは既知のコンピュータウィルスのコードの中からこのウィルスに固有のコードパターンを「ウィルス定義ファイル」と呼ばれるファイルに記憶しておき、このウィルス定義ファイル内のコードパターンと検索対象のファイルのコードとを比較してコンピュータウィルスの存在を検出するというもの

である。

【０００４】

このパターンマッチング方式は、より迅速にコンピュータウィルスを検出できるという点で優れているが、新たなコンピュータウィルスが出現する度にこれを１つ１つ解析してコードパターンを抽出するという事前処理が必要となるため、新種のコンピュータウィルスに対しては対応が遅れてしまうという問題がある。

そこで、ワクチンソフトの提供者は、最新のコンピュータウィルスに対応したウィルス定義ファイルを自身のホームページ上に用意しておき、ユーザはこのホームページにアクセスして自身のワクチンソフトをアップデートする等して、この問題に対処している。しかし、ユーザからみれば、このようなアップデート作業は非常に煩わしいものである。

【０００５】

また、ジャンクメールについても、既知のジャンクメールの類型パターンを記憶しておき、これと照合してジャンクメールを検出するというような対応策が考えられる。しかし、これも上記コンピュータウィルスと同様の問題が生じてしまう。

【０００６】

本発明は、このような背景の下になされたものであり、ユーザの利便性を損ねることなく、インターネット等のコンピュータネットワークにおいて様々な不正行為による被害を防止するためのデータ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体に関する。

【０００７】

【課題を解決するための手段】

上述した課題を解決するため、本発明は、データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置が、受信したデータを予め定められたサーバに転送するステップと、

前記サーバが、前記データ中継装置から転送されてくるデータを受信し、当該データの宛先へ送信するステップと、

前記サーバが、前記送信したデータに応答して前記宛先から送信されてくる応

答データを受信するステップと、

前記サーバが、前記宛先から受信した応答データに対してセキュリティチェックを行うステップと、

前記サーバが、前記セキュリティチェックを行った後の応答データを前記データ中継装置を介して前記情報通信装置に送信するステップと

を備えるデータ通信方法を提供する。

この方法によれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに応答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うことができる。

【０００８】

また、本発明は、データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置が、受信したデータを予め定められたサーバに転送するステップと、

前記サーバが、前記データ中継装置から転送されてくるデータを受信するステップと、

前記サーバが、前記受信したデータに対してセキュリティチェックを行うステップと、

前記サーバが前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するステップと

を備えるデータ通信方法を提供する。

この方法によれば、データ中継装置によって転送されてくるデータを受信すると、受信したデータに対してセキュリティチェックを行うことができる。

【０００９】

また、本発明は、データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置と、データに対してセキュリティチェックを行うサーバとからなるデータ通信システムであって、

前記データ中継装置が、

受信したデータを前記サーバに転送する転送手段を備え、

前記サーバが、

前記データ中継装置から転送されてくるデータを受信するデータ受信手段と、

前記受信したデータを当該データの宛先へ送信するデータ送信手段と、

前記送信したデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信手段と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後の応答データを前記データ中継装置を介して前記情報通信装置に送信する応答データ送信手段と

を備えるデータ通信システムを提供する。

このシステムによれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに応答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うことができる。

【００１０】

また、本発明は、データ通信を行う情報通信装置に接続されてデータ伝送を中継するデータ中継装置と、データに対してセキュリティチェックを行うサーバとからなるデータ通信システムであって、

前記データ中継装置が、

受信したデータを前記サーバに転送する転送手段を備え、

前記サーバが、

前記データ中継装置から転送されてくるデータを受信するデータ受信手段と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信手段と

を備えるデータ通信システムを提供する。

このシステムによれば、データ中継装置によって転送されてくるデータを受信すると、受信したデータに対してセキュリティチェックを行うことができる。

【００１１】

また、本発明は、データの送受信を行って当該データの伝送を中継する通信手段と、

前記通信手段によって受信された受信データを、転送されてきたデータに対してセキュリティチェックを行うサーバへ前記通信手段を用いて転送する転送手段と

を備えるデータ中継装置を提供する。

この装置によれば、セキュリティチェックを行うサーバへ受信データを転送先へ転送することができる。

【００１２】

また、本発明は、データの送受信を行って当該データの伝送を中継する通信手段と、

自装置に固定的に割り当てられ、自装置を他のデータ中継装置と識別するための装置識別情報を記憶する記憶手段を備え、

前記通信手段によって受信された受信データに対して前記記憶手段に記憶されている装置識別情報を付加し、当該装置識別情報が付加された受信データを予め定められた転送先へ前記通信手段を用いて転送する転送手段と

を備えるデータ中継装置を提供する。

この装置によれば、受信データに装置識別情報を付加して予め定められた転送先へ転送することができる。

【００１３】

また、本発明は、データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信手段と、

前記受信したデータを当該データの宛先へ送信するデータ送信手段と、

前記データ送信手段によって送信されたデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信手段と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後の応答データを前記情報通信装置に送信

する応答データ送信手段と

を備えるサーバを提供する。

このサーバによれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに応答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うことができる。

【００１４】

また、本発明は、データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信手段と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェック手段と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信手段と

を備えるサーバを提供する。

このサーバによれば、データ中継装置によって転送されてくるデータを受信すると、受信したデータに対してセキュリティチェックを行うことができる。

【００１５】

また、本発明は、コンピュータに、

データの送受信を行って当該データの伝送を中継する通信機能と、

前記通信機能によって受信された受信データを、転送されてきたデータに対してセキュリティチェックを行うサーバへ前記通信機能を用いて転送する転送機能と

を実行させるためのプログラムを提供する。

このプログラムによれば、セキュリティチェックを行うサーバへ受信データを転送することができる。

【００１６】

また、本発明は、コンピュータに、

データの送受信を行って当該データの伝送を中継する通信機能と、

自装置に固定的に割り当てられ、自装置を他のデータ中継装置と識別するため

の装置識別情報を記憶する記憶機能と、

前記通信機能によって受信された受信データに対して前記記憶機能によって記憶されている装置識別情報を付加し、当該装置識別情報が付加された受信データを予め定められた転送先へ前記通信機能を用いて転送する転送機能と

を実行させるためのプログラムを提供する。

このプログラムによれば、受信データに対して装置識別情報を付加し、この装置識別情報が付加された受信データを予め定められた転送先へ転送することができる。

【００１７】

また、本発明は、コンピュータに、

データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信機能と、

前記受信したデータを当該データの宛先へ送信するデータ送信機能と、

前記データ送信機能によって送信されたデータに応答して前記宛先から送信されてくる応答データを受信する応答データ受信機能と、

前記受信した応答データに対してセキュリティチェックを行うセキュリティチェック機能と、

前記セキュリティチェックを行った後の応答データを前記情報通信装置に送信する応答データ送信機能と

を実行させるためのプログラムを提供する。。

このプログラムによれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに応答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うことができる。

【００１８】

また、本発明は、コンピュータに、

データ通信を行う情報通信装置から送信され、データ中継装置によって転送されてくるデータを受信するデータ受信機能と、

前記受信したデータに対してセキュリティチェックを行うセキュリティチェッ

ク機能と、

前記セキュリティチェックを行った後のデータを当該データの宛先へ送信するデータ送信機能と

を実行させるためのプログラムを提供する。

このプログラムによれば、データ中継装置によって転送されてくるデータを受信すると、受信したデータに対してセキュリティチェックを行うことができる。

【００１９】

【発明の実施の形態】

以下、図面を参照して、この発明の実施形態について説明する。ただし、本発明は、かかる実施形態に限定されず、その技術思想の範囲内で種々の変更が可能である。

【００２０】

Ａ：構成

まず、実施形態の構成について説明する。

（１）システムの全体構成

図１は、実施形態に係るシステムの全体構成を示すブロック図である。図１に示すように、このシステムは、ホームネットワーク１、ＡＤＳＬ（Asymmetric Digital Subscriber Line）網２、インターネットサービスプロバイダ（以下ＩＳＰと略称）３、インターネット４、センタ５及びWWWサーバ６を備えている。なお、図１においては、システム構成を簡単に説明するために、ホームネットワーク１、ＩＳＰ３及びWWWサーバ６をそれぞれ１つしか図示していないが、実際にはこれらの構成要素はそれぞれ複数存在している。

【００２１】

ホームネットワーク１は、ユーザの家庭に設置されたローカルエリアネットワークである。このホームネットワーク１は、各種の情報通信装置１０～１３、ルータ１４、ＡＤＳＬモデム１５、及びこれらを接続する各種通信ケーブルを備えている。図１では情報通信装置の一例として、パーソナルコンピュータ（以下ＰＣと略称）１０、テレビジョン１１、ＭＰ３（MPEG-1 Audio Layer-3）プレーヤ１２、ＰＤＡ（Personal Digital Assistants）１３を示しているが、この

他にも例えばデジタルカメラ、ゲーム用機器、セットトップボックス、携帯電話機、冷蔵庫、電子レンジ、防犯システム等の様々な機器を利用することが可能である。これら情報通信装置１０～１３は、WWW（World Wide Web）ブラウザ等の文書閲覧プログラムを搭載しており、インターネット４に接続された各種サーバが提供する情報を取得し表示することが可能になっている。

【００２２】

ルータ１４は、ツイストペアケーブル（例えば１０ＢＡＳＥ－Ｔケーブル）や同軸ケーブル等の通信ケーブルによって情報通信装置１０～１３に接続されるとともに、モジュラーケーブル等の通信ケーブルを介してＡＤＳＬモデム１５に接続されている。このルータ１４は、自身が記憶しているルーティングテーブルに基づいてデータ伝送を中継する周知のルーティング機能を備える他、所定の条件に基づいて中継対象のデータをセンタ５に転送する転送機能を備えている。

ここで、ルータ１４は、上記転送機能を実現する際に、センタ５内に設置されたセキュリティサーバ５１（後述する）を情報通信装置１０～１３の代理となるプロキシサーバに指定し、このセキュリティサーバ５１に対していわゆるトンネリングを行ってデータ転送を行うようになっている。

【００２３】

ＡＤＳＬモデム１５は、モジュラーケーブル等の通信ケーブルを介してＡＤＳＬ網２に接続されている。このＡＤＳＬモデム１５は、ＡＤＳＬ網２とホームネットワーク１との間でデータ信号の授受が可能となるように、このデータ信号の変復調を行う機能を備えている。

【００２４】

センタ５は、図示せぬルータを介してインターネット４に接続されている。このセンタ５は、セキュリティサーバ５１、シリアル情報データベース（以下データベースをＤＢと略称）５２、セキュリティ契約情報ＤＢ５３、及びこれらを相互に接続する高速デジタル回線５４を備えている。

【００２５】

セキュリティサーバ５１は、プロキシ機能とセキュリティチェック機能を備えたサーバである。

プロキシ機能とは、前述したように、ルータ１４からＡＤＳＬ網２及びインターネット４を介して転送されてくるデータを受信すると、受信したデータを情報通信装置１０～１３の代理としてその宛先に送信し、これに応答してその宛先から送信されてくるデータを受信し、これを情報通信装置１０～１３に送信する機能である。

セキュリティチェック機能とは、パターンマッチング等を行ってコンピュータウィルスやジャンクメールを検出し、検出したコンピュータウィルスを周知のアルゴリズムを用いて駆除したり、ジャンクメールを廃棄したりする機能である。この際用いられるコンピュータウィルスの駆除方法としては、コンピュータウィルスに相当するコードを適当なコードに置き換えたり、コンピュータウィルスに感染したデータファイルを削除したり、そのファイルの拡張子を変更したりする等の方法がある。

さらに、このセキュリティサーバ５１は、情報通信装置１０～１３のユーザがセキュリティチェックを受ける契約を行うための契約申込画面を示すデータ（以下契約申込画面データと呼ぶ）を記憶しており、情報通信装置１０～１３からのリクエストに応じて、この契約申込画面データを送信する機能を備えている。

【００２６】

シリアル情報ＤＢ５２には、既に製造された全てのルータ１４のシリアルナンバーと、これらルータ１４の各々に予め割り当てられている個体パスワードとからなるシリアル情報が格納されている。このシリアル情報は、セキュリティサーバ５１がルータ１４の正当性を確認するために利用される。

【００２７】

セキュリティ契約情報ＤＢ５３には、情報通信装置１０～１３のユーザとセンタ５の管理者との間で交わされるセキュリティチェックの契約の内容を示すセキュリティ契約情報が格納されている。より具体的には、このセキュリティ契約情報は、各ルータ１４から転送されてくるデータに対し、どのような種類のセキュリティチェックを行うかということを示す情報である。

【００２８】

ＩＳＰ３は、図示せぬルータを介してＡＤＳＬ網２に接続されるとともに、図

示せぬ別のルータを介してインターネット４に接続されている。このＩＳＰ３は、図１に示したＰＯＰサーバ３１、ＩＭＡＰサーバ３２、ＳＭＴＰサーバ３３、契約代行サーバ３４、ユーザ情報ＤＢ３５、課金情報ＤＢ３６、及びこれらを接続する高速デジタル回線３７のほか、図示せぬゲートウェイサーバやＤＮＳ（Domain Name Service）サーバを備えている。

このＩＳＰ３は、上述したサーバ群やデータベース群が連携して機能することにより、情報通信装置１０～１３に対し、インターネット４への接続サービスや電子メールの中継サービスを提供する。さらに、ＩＳＰ３は、情報通信装置１０～１３のユーザとセンタ５と間で交わされるべきセキュリティチェックの契約に関する処理をセンタ５に代わって行う契約代行機能と、このセキュリティチェックに関する課金処理をセンタ５に代わって行う課金代行機能を備えている。

【００２９】

以下、ＩＳＰ３を構成するサーバ及びデータベースの各々が実現する機能の概略を説明する。

まず、ＰＯＰサーバ３１、ＩＭＡＰサーバ３２及びＳＭＴＰサーバ３３はそれぞれ周知のサーバである。即ち、ＰＯＰサーバ３１はＰＯＰ３（Post Office Protocol version 3）を用いて情報通信装置１０～１３宛の電子メール（以下受信メール）をその宛て先に配信するサーバである。ＩＭＡＰサーバ３２はＩＭＡＰ４（Internet Message Access Protocol version 4）を用いて情報通信装置１０～１３宛の受信メールをその宛先に配信するサーバである。ＳＭＴＰサーバ３３は、ＳＭＴＰ（Simple Mail Transfer Protocol）を用いて情報通信装置１０～１３から送信された電子メール（以下送信メール）をその宛先に対応したＳＭＴＰサーバ（図示略）へ転送するサーバである。

【００３０】

次に、契約代行サーバ３４は、前述したセキュリティチェックの契約代行を行うサーバである。より具体的には、契約代行サーバ３４は、情報通信装置１０～１３から送信されてくるセキュリティ契約情報を受信すると、ユーザ認証を行ってユーザの正当性を確認した後、そのセキュリティ契約情報を本来の契約主体であるセンタ５に転送するとととともに、当該セキュリティ契約情報をＩＳＰ３内の

ユーザ情報ＤＢ３５に転送するようになっている。

【００３１】

ユーザ情報ＤＢ３５には、ＩＳＰ３によるＩＰ接続サービスやメール中継サービスを受けるユーザの属性情報に加え、上述のようにして契約代行サーバ３５から転送されてくるセキュリティ契約情報が記憶されている。

【００３２】

課金情報ＤＢ３６には、ＩＳＰ３によるＩＰ接続サービスやメール中継サービスに対応した課金情報に加えて、センタ５が行うセキュリティチェックに対応した課金情報が記憶されている。この課金情報ＤＢ３６は、専用線を介して金融機関システム７に接続されている。金融機関システム７は、課金情報ＤＢ３６に記憶されている課金情報に基づいて、ユーザが指定する銀行口座から課金額を引き落とす処理を行うようになっている。

【００３３】

WWWサーバ６は、図示せぬルータを介してインターネット４に接続されている。このWWWサーバ６は、各種コンテンツを示すコンテンツデータをＨＴＭＬ（HyperText Markup Language）形式やＸＭＬ（Extensible Markup Language）形式で記憶しており、インターネット４を介して送信されてくるＨＴＴＰ（HyperText Transfer Protocol）リクエストに応答して、これらコンテンツデータをＨＴＴＰレスポンスとして送信するようになっている。

ここで、コンテンツとは、例えばニュース、電子書籍、オーディオ、ビデオクリップ、ホームページというような、テキスト、音楽、画像の少なくともいずれか１つによって表現される情報を意味する他、ゲームソフトやＪａｖａ（登録商標）アプレット等の各種コンピュータプログラムをも含む概念である。

【００３４】

（２）ルータ１４の構成

次に、図２のブロック図を参照しながら、ルータ１４の構成について説明する。

図２に示すように、ルータ１４は、ＣＰＵ（Central Proccessing Unit）１４１、ＲＯＭ（Read Only Memory）１４２、ＲＡＭ（Random Access Memory）１４

３、フラッシュメモリ１４４、表示部１４５、ＬＡＮ通信部１４６、ＷＡＮ通信部１４７、及びこれらを相互に接続するバス１４８を備えている。

ＲＯＭ１４２には、ルーティング処理を行うためのルーティングプログラム等の制御プログラムの他、各ルータ１４に固有のシリアルナンバーや、このシリアルナンバーに基づいて生成された個体パスワードが記憶されている。この個体パスワードは、シリアルナンバーを構成する文字列を基に所定のアルゴリズムに従って生成される文字列であり、ルータ１４の製造時にシリアルナンバーとともにＲＯＭ１４２に書き込まれる。

ＣＰＵ１４１は、ＲＯＭ１４２から制御プログラムを読み出し、これを実行することによってルータ１４全体を制御する。ＲＡＭ１４３は、ＣＰＵ１４１のワークエリアとして用いられ、例えばＣＰＵ１４１によって実行される制御プログラムが展開されたり、制御プログラムの実行時に用いられる各種データが一時的に記憶される。

フラッシュメモリ１４４には、ルーティング先のＩＰアドレスが記述された周知のルーティングテーブルと、ルータ１４のＩＰアドレスと、セキュリティサーバ５１のＩＰアドレスと、セキュリティサーバ５１に転送すべきデータが従うアプリケーション層プロトコルのプロトコル名が記述されたチェック対象プロトコルテーブルが記憶されている。これらフラッシュメモリ１４４に記憶されるもののうち、セキュリティサーバ５１のＩＰアドレスと、チェック対象プロトコルテーブルに記述されるデータは、ユーザがセキュリティチェックの契約を締結することにより、契約代行サーバ３４からＡＤＳＬ網２を介して通知されて、このフラッシュメモリ１４４に記憶されるようになっている。

表示部１４５は、図示せぬＬＥＤ（Light Emitting Diode）や液晶パネル等の表示装置と、これを駆動する駆動ドライバとを備えており、ＣＰＵ１４１の制御の下で各種の状態や情報を表示するようになっている。

ＬＡＮ通信部１４６は、図示せぬ４ポートハブを備えている。この４ポートハブには、各情報通信装置１０～１３に接続される通信ケーブルの端部が挿入され、これにより、各情報通信装置１０～１３とルータ１４とが相互に接続されるようになっている。ＬＡＮ通信部１４６、この４ポートハブを介して、情報通信装

置１０～１３との間でデータ通信を行う。

ＷＡＮ通信部１４７は、図示せぬＡＤＳＬポートを備えている。このＡＤＳＬポートには、ＡＤＳＬモデム１５に接続される通信ケーブルの端部が挿入され、これにより、ＡＤＳＬモデム１５とルータ１４とが接続されるようになっている。ＷＡＮ通信部１４７は、このＡＤＳＬポートを介して、ＡＤＳＬモデム１５との間でデータ通信を行う。

【００３５】

ここで、図３のフォーマット図を参照しながら、フラッシュメモリ１４４に記憶されているチェック対象プロトコルテーブルの構成について説明する。

図３に示すように、チェック対象プロトコルテーブルには、セキュリティチェックの対象となるアプリケーション層プロトコルのプロトコル名と、このアプリケーション層プロトコルに対応する宛先ポート番号とが関連付けて記憶されている。ルータ１４のＣＰＵ１４１は、中継すべきパケットのＴＣＰヘッダに含まれている宛先ポート番号が、チェック対象プロトコルテーブルに記憶されている宛先ポート番号と一致した場合には、そのパケットをセキュリティサーバ５１に転送する。

一方、中継すべきパケットのＴＣＰヘッダに含まれている宛先ポート番号が、チェック対象プロトコルテーブルに記憶されている宛先ポート番号と一致しない場合には、ＣＰＵ１４１は、通常のルーティング処理を行う。即ち、ＣＰＵ１４１は、パケットのＩＰヘッダに書き込まれているＩＰアドレスと、フラッシュメモリ１４４内のルーティングテーブルとに従って当該パケットをその宛先へ送信するようになっている。

図３に示す例では、ＰＯＰ３、ＳＭＴＰ、ＨＴＴＰという３種類のアプリケーション層プロトコルのデータをセキュリティサーバ５１に転送するように設定されており、これらアプリケーション層プロトコルに対応する宛先ポート番号はそれぞれ「１１０」、「２５」、「８０」であることを意味している。

【００３６】

（３）センタ５の構成

次に、センタ５の構成について詳細に説明する。

（３－１）セキュリティサーバ５１の構成

まず、図４のブロック図を参照しながら、セキュリティサーバ５１の構成について説明する。

図４に示すように、セキュリティサーバ５１は、ＣＰＵ５１１、ＲＯＭ５１２、ＲＡＭ５１３、通信部５１４、ハードディスク装置５１５、及びこれらを相互に接続するバス５１６を備えている。

ＲＯＭ５１２にはＩＰＬ（Initial Program Loader）等の基本制御を司る制御プログラムが格納されている。ＣＰＵ５１１は、このＲＯＭ５１２やハードディスク装置５１５から各種プログラムを読み出し、これを実行する。ＲＡＭ５１３は、ＣＰＵ５１１のワークエリアとして用いられ、例えばＣＰＵ５１１によって実行されるプログラムが展開されたり、プログラム実行時に用いられる各種データが一時的に記憶される。

通信部５１４は、インターネット４に接続するための接続インタフェースやモデムを備えており、インターネット４を介して各種の通信装置とデータ通信を行う。

ハードディスク装置５１５には、図４に示す契約申込画面配信プログラムやセキュリティチェックプログラムの他、情報通信装置１０～１３のプロキシサーバとして機能するための図示せぬプロキシプログラムが記憶されている。契約申込画面配信プログラムは、前述した契約申込画面データを情報通信装置１０～１３に配信するためのコンピュータプログラムである。ＣＰＵ５１１は、情報通信装置１０～１３のいずれかからの要求に応じて、この契約申込画面配信プログラムを実行し、要求元の情報通信装置１０～１３に対して契約申込画面データを送信するようになっている。セキュリティチェックプログラムは、セキュリティサーバ５１が情報通信装置１０～１３の代理として送受信するデータに対してセキュリティチェックを行うためのコンピュータプログラムである。このセキュリティチェックプログラムは、新種のコンピュータウィルス等に対応可能となるように、センタ５の管理者によって随時更新されている。

【００３７】

（３－２）シリアル情報ＤＢ５２の構成

次に、図５のフォーマット図を参照しながら、シリアル情報ＤＢ５２の構成について説明する。

図５に示すように、シリアル情報ＤＢ５２には、シリアルナンバーと、このシリアルナンバーに基づいて生成された個体パスワードとが対応付けて記憶されている。図５に示す例では、シリアルナンバー「Ｓ０００００１」に対応する個体パスワードが「ａｂｃ１２３」であることを意味している。これらのシリアル情報は、ルータ１４の製造工場から通知されることにより、このシリアル情報ＤＢ５２に格納されるようになっている。

【００３８】

（３－３）セキュリティ契約情報ＤＢ５３の構成

次に、図６のフォーマット図を参照しながら、セキュリティ契約情報ＤＢ５３の構成について説明する。

図６に示すように、セキュリティ契約情報ＤＢ５３には、各ルータ１４の「シリアルナンバー」に対応して、そのルータ１４のユーザが契約によって指定した「セキュリティチェックの内容」が記憶されている。図６に示す例では、シリアルナンバー「Ｓ０００００１」に対応するルータ１４に対しては、コンピュータウィルスの駆除を目的とした「ウィルスチェック」と、ジャンクメールの廃棄を目的とした「ジャンクメールチェック」とが「オン」設定されており、これらウィルスチェック及びジャンクメールチェックがなされることを意味している。

さらに、このシリアルナンバー「Ｓ０００００１」に対応するルータ１４において、ウィルスチェックのチェック対象プロトコルは、「ＰＯＰ３」、「ＳＭＴＰ」、「ＨＴＴＰ」となっている。これは、情報通信装置１０～１３がＰＯＰ３を用いて受信する受信メールと、情報通信装置１０～１３がＳＭＴＰを用いて送信する送信メールと、WWWサーバ６から情報通信装置１０～１３に対しＨＴＴＰレスポンスとして送信されるコンテンツデータに対してウィルスチェックがなされることを意味している。同様に、ジャンクメールチェックのチェック対象プロトコルは「ＰＯＰ３」となっており、これは、情報通信装置１０～１３がＰＯＰ３を用いて受信する受信メールに対してジャンクメールチェックがなされることを意味している。

これらのセキュリティ契約情報は、契約代行サーバ３４から通知されることにより、このセキュリティ契約情報ＤＢ５３に記憶されるようになっている。

【００３９】

（４）ＩＳＰ３の構成

次に、ＩＳＰ３内に設置されているユーザ情報ＤＢ３５及び課金情報ＤＢ３６の構成について説明する。

（４－１）ユーザ情報ＤＢ３５の構成

図７は、ユーザ情報ＤＢ３５に記憶されているユーザ情報の一例を示したフォーマット図である。

図７に示すように、ユーザ情報ＤＢ３５には、ＩＳＰ３が各ユーザに割り当てた「ユーザＩＤ」と「パスワード」、ユーザが使用するルータ１４の「シリアルナンバー」とこれに対応する「個体パスワード」、このルータ１４に対応した「セキュリティチェックの内容」の他、「ユーザ名」、「住所」、「生年月日」等のユーザの属性情報が、それぞれ関連付けて記憶されている。

例えば図７に示すユーザＩＤ「ａａａ」に対応するユーザについては、図６で説明したシリアルナンバー「Ｓ０００００１」のルータ１４に対応するセキュリティチェックの内容と同一のデータが記憶されている。一方、ユーザＩＤ「ｂｂｂ」が示すユーザについては、セキュリティチェックの内容がブランクになっており、このユーザはセキュリティチェックの契約を行っていないことが示されている。

上記の「シリアルナンバー」、「個体パスワード」及び「セキュリティチェックの内容」は、前述したように、契約代行サーバ３４から通知されることにより、このユーザ情報ＤＢ３５に記憶されるようになっている。

【００４０】

（４－２）課金情報ＤＢ３６の構成

次に、図８のフォーマット図を参照しながら、課金情報ＤＢ３６の構成を説明する。

図８に示すように、課金情報ＤＢ３６には、ＩＳＰ３のユーザに割り当てられた「ユーザＩＤ」に対応して、このユーザに対して課された課金額を引き落とす

ための「銀行口座」、ＩＳＰ３が提供した接続サービス及びメール中継サービスに対してユーザが毎月支払うべき「ＩＳＰ課金額」、センタ５が行ったセキュリティチェックに対してユーザが毎月支払うべき「セキュリティチェック課金額」、およびこれらの課金額を合算した「課金額合計」が記憶されている。例えば、ユーザＩＤ「ａａａ」に対応するユーザに対しては、ＩＳＰ課金額「５０００円」とセキュリティチェック課金額「３０００円」とを合算した「８０００円」が毎月、課金されることを意味している。

ここで、ウィルスチェックとジャンクメールチェックとでは別々に課金されるようになっており、図８に示す例では、ウィルスチェックに関する課金額は「２０００円」であり、ジャンクメールチェックに関する課金額は「１０００円」に設定されている。

また、ユーザＩＤ「ｂｂｂ」に対応するユーザは、ＩＳＰ３によるサービスのみを受けており、センタ５によるセキュリティチェックを受けていないので、セキュリティチェック課金額はブランクになっている。

このような課金情報は、ＩＳＰ３が図示せぬ記憶装置に記憶している当該ＩＳＰ３自身のサービス契約情報と、上述したユーザ情報ＤＢ３５に記憶されているセキュリティチェックに関する情報とに基づいて生成され、この課金情報ＤＢ３６に格納される。

以上が本実施形態の構成である。

【００４１】

Ｂ：動作

次に、上記構成からなる実施形態の動作について説明する。

前述したように、ルータ１４は受信したデータをトンネリングを行ってセキュリティサーバに転送し、これに応じて、セキュリティサーバ５１は情報通信装置１０～１３のプロキシサーバとして機能する。

そこで、具体的な動作例を説明する前に、ルータ１４とセキュリティサーバ５１がデータを送受信する際に行う基本動作を、送受信されるデータの構造とともに説明しておく。

【００４２】

図９は、ＰＣ１０が、ＰＯＰサーバ３１、ＩＭＡＰサーバ３２、ＳＭＴＰサーバ３３及びWWWサーバ６のいずれかとデータ通信を行う際の仕組みを説明する説明図である。なお、ＰＣ１０が、ＰＯＰサーバ３１、ＩＭＡＰサーバ３２、ＳＭＴＰサーバ３３及びWWWサーバ６のいずれかとデータ通信を行う際には、送受信の対象となるデータは複数のパケットに分割されて送受信されるが、図９においては簡単に説明するため、これら複数のパケットのうちの１つのパケットのみに着目して説明を行う。

【００４３】

図９において、まず、ＰＣ１０は、ＰＯＰサーバ３１、ＩＭＡＰサーバ３２、ＳＭＴＰサーバ３３、WWWサーバ６のいずれか（以下ＰＯＰサーバ３１を例示して説明する）に対して各種要求を行うためのパケットＰ１を送信する。このパケットＰ１は、図１０のフォーマット図に示すように、ＩＰヘッダの宛先アドレスフィールドには「ＰＯＰサーバ３１のＩＰアドレス」が記述され、送信元アドレスフィールドには「ＰＣ１０のＩＰアドレス」が記述されている。また、ＴＣＰヘッダの宛先ポート番号フィールドには「１１０」番が記述されている。

【００４４】

ルータ１４は、パケットＰ１を受信すると、カプセル化を行ってパケットＰ２を生成し、これをセキュリティサーバ５１に送信する。このパケットＰ２は、図１１のフォーマット図に示すように、パケットＰ１に対してさらにＩＰヘッダ、ＴＣＰヘッダ及びＴＣＰペイロードが付加されたデータ構造となっている。

付加されたＩＰヘッダの宛先アドレスフィールドには「セキュリティサーバ５１のＩＰアドレス」が記述され、送信元アドレスフィールドには「ルータ１４のＩＰアドレス」が記述されている。

ここで、本実施形態では、ルータ１４及びセキュリティサーバ間はＳＯＣＫＳプロトコルを用いてトンネリングを行うようになっている。そこで、付加されたＴＣＰヘッダには、ＳＯＣＫＳプロトコルにおいて使用する宛先ポート番号フィールドが設けられており、このフィールドには「１０５０」番が記述されている。さらに、付加されたＴＣＰペイロードには、トンネル用認証情報フィールドが設けられており、このフィールドにはルータ１４のフラッシュメモリ１４４から

読み出された「シリアルナンバー」が記述されている。

【００４５】

セキュリティサーバ５１はパケットＰ２を受信すると、まず、ＴＣＰペイロードに含まれるシリアルナンバーがシリアル情報ＤＢ５２に記憶されているか否かによりルータ１４の正当性を確認する。次いで、セキュリティサーバ５１は、ルータ１４によって付加されたＩＰヘッダ、ＴＣＰヘッダ及びＴＣＰペイロードを取り除いて脱カプセル化を行い、パケットＰ３を得る。さらに、セキュリティサーバ５１は、このパケットＰ３のＩＰヘッダの送信元アドレスフィールドに書きこまれている「ＰＣ１０のＩＰアドレス」を、「セキュリティサーバ５１のＩＰアドレス」に書き換えて、図１２のフォーマット図に示すようなパケットＰ４を生成し、これをＰＯＰサーバ３１に送信する。

【００４６】

ＰＯＰサーバ３１はパケットＰ４を受信すると、これに応答して、ＰＣ１０宛のデータを含むパケットＰ５をセキュリティサーバ５１に送信する。このパケットＰ５においては、図１３のフォーマット図に示すように、ＩＰヘッダの宛先アドレスフィールドに「セキュリティサーバ５１のＩＰアドレス」が記述され、送信元アドレスフィールドには「ＰＯＰサーバ３１のＩＰアドレス」が記述されている。また、ＴＣＰヘッダの送信元ポート番号フィールドには「１１０」番が記述されている。

【００４７】

セキュリティサーバ５１は、パケットＰ５を受信するとＩＰヘッダの宛先アドレスフィールドの「セキュリティサーバ５１のＩＰアドレス」を「ＰＣ１０のＩＰアドレス」に書き換え、送信元アドレスフィールドの「ＰＯＰサーバ３１のＩＰアドレス」を「セキュリティサーバ５１のＩＰアドレス」に書き換える。さらに、セキュリティサーバ５１は、書き換え後のパケットＰ５に対してカプセル化を行ってパケットＰ６を生成し、これをＰＣ１０に送信する。

このパケットＰ６においては、図１４のフォーマット図に示すように、カプセル化によって付加されたＩＰヘッダの宛先アドレスフィールドに「ルータ１４のＩＰアドレス」が記述され、送信元アドレスフィールドには「セキュリティサー

バ５１のＩＰアドレス」が記述されている。また、付加されたＴＣＰヘッダの送信元ポート番号フィールドには「１０５０」番が記述されている。

【００４８】

ルータ１４は、パケットＰ６を受信すると、脱カプセル化を行ってパケットＰ７を得て、このパケットＰ７をＰＣ１０に送信する。

【００４９】

このように、ルータ１４とセキュリティサーバ５１は、中継すべきパケットに対してカプセル化やＩＰアドレスの書き換え等を適宜行うことにより、データの中継処理を実行している。

なお、上記の例では、ＰＣ１０とＰＯＰサーバ３１とがデータ通信を行う場合を説明したが、ＰＣ１０以外の他の情報通信装置１１～１３がその処理主体であってもＰＣ１０と動作は共通である。

【００５０】

次に、具体的な動作例について説明する。

本実施形態では、まず、ユーザがセキュリティチェックを受けるための契約を締結し、この契約が締結された後に、各プロトコルに応じたセキュリティチェックが実施されることになる。

そこで、以下では、（１）セキュリティチェックの契約、について説明した後、各プロトコルに応じた動作例として、（２）ＰＯＰ３を用いた受信メールに対するセキュリティチェック、（３）ＳＭＴＰを用いた送信メールに対するセキュリティチェック、（４）ＨＴＴＰを用いたコンテンツデータに対するセキュリティチェック、について説明する。

【００５１】

（１）セキュリティチェックの契約

まず、図１５に示すシーケンスを参照しながら、ユーザがセキュリティチェックの契約を締結する際の動作について説明する。

ユーザは、ルータ１４を購入すると、通信ケーブルを用いてルータ１４と情報通信装置１０～１３及びＡＤＳＬモデム１５とを接続する。次いで、ユーザは、ルータ１４に対し初期設定を行うべく、ＰＣ１０等を操作してWWWブラウザを

起動させ、このWWWブラウザによって表示される対話画面を参照しながら所定の操作を行う。これに応じてＰＣ１０からルータ１４に対して設定通知がなされ、ルータ１４は、自身のＩＰアドレスをフラッシュメモリ１４４に記憶したり、ルーティングテーブルにルーティング先のＩＰアドレスを書き込む等の処理を行う。このような初期設定が完了すると、ルータ１４は、データをルーティング可能な状態になる。

【００５２】

次いで、ユーザは、WWWブラウザによって表示された対話画面の所定フィールド内に、ルータ１４の仕様書等に記載されているＵＲＬ（Uniform Resource Locator）を入力する。ＰＣ１０はこの入力操作を受け付けると（ステップＳ１）、ＧＥＴメソッドを用いたＨＴＴＰリクエストを契約申込画面要求としてセキュリティサーバ５１に送信する（ステップＳ２）。この契約申込画面要求には、ユーザによって入力されたＵＲＬが含まれており、このＵＲＬは契約申込画面データを記憶しているセキュリティサーバ５１のリソースを示している。

この契約申込画面要求は、ルータ１４のルーティング機能によってＡＤＳＬ網２に送出された後、図示せぬゲートウェイやルータを次々と経由してセキュリティサーバ５１によって受信される。

【００５３】

セキュリティサーバ５１は、上記契約申込画面要求を受信すると、これに応じて契約申込画面配信プログラムを起動する。そして、セキュリティサーバ５１は、受信した契約申込画面要求に含まれるＵＲＬによって指定されるリソースから契約申込画面データを読み出し、これをＨＴＴＰレスポンスとしてＰＣ１０に送信する（ステップＳ３）。

【００５４】

ＰＣ１０は、インターネット４及びＡＤＳＬ網２を介して上記契約申込画面データを受信すると、これを解釈して図示せぬディスプレイ装置に契約申込画面を表示する（ステップＳ４）。

このとき表示される契約申込画面の一例を図１６の模式図に示す。図１６に示すように、この契約申込画面には、ユーザが加入しているＩＳＰ名を入力するた

めのフィールドＦ１と、ルータ１４のシリアルナンバーを入力するためのフィールドＦ２と、個体パスワードを入力するためのフィールドＦ３と、ＩＳＰ３によって割り当てられたユーザＩＤを入力するためのフィールドＦ４と、ユーザＩＤに対応したパスワードを入力するためのフィールドＦ５と、所望するセキュリティチェックを選択するためのチェックボックスＦ６～Ｆ１２とが設けられている。また、フィールドＦ１の右方には、プルダウンメニューボックスＭＢが設けられており、ユーザがこのプルダウンメニューボックスＭＢをマウスでクリックすると、「Ａ社、Ｂ社、Ｃ社、・・・」というように各ＩＳＰ名がプルダウンで列記表示され、ユーザはこの中から自身が加入するＩＳＰ３を選択することができる。さらに、このＩＳＰ名には、対応するＩＳＰ３が備える契約代行サーバ３４のＩＰアドレスが関連付けられている。

図１６に示すように、ユーザが各フィールドＦ１～Ｆ１２にデータを入力した後、「送信」と表記されたソフトボタンＳＢをマウスでクリックすると、ＰＣ１０はこの操作を受け付ける（ステップＳ５）。

次いで、ＰＣ１０は、ユーザによって入力されたＩＳＰ名に関連付けられている契約代行サーバ３４のＩＰアドレスを宛先として、ユーザによってフィールドＦ１～Ｆ１２に入力されたデータを含むＨＴＴＰリクエストを契約要求として送信する（ステップＳ６）。

【００５５】

ＩＳＰ３の契約代行サーバ３４は、上記契約要求を受信すると、まず、受信した契約要求の中からユーザＩＤ及びパスワードを抽出し、これらがユーザ情報ＤＢ３５に記憶されているものと一致するか否かを判断することにより、ユーザ認証を行う（ステップＳ７）。ここでは、契約要求に含まれるユーザＩＤ「ａａａ」及びパスワード「ｘｘｘｚｚｚ」は、図７に示すユーザ情報ＤＢ３５に記憶されたものと一致するので、ユーザは正当であると判断されることになる。

【００５６】

ステップＳ７において正当なユーザであると判断された場合には、契約代行サーバ３４は、上記契約要求に含まれるユーザＩＤ及びパスワード以外のデータ（即ちセキュリティ契約情報）をユーザ情報ＤＢ３５に転送し、このユーザ情報Ｄ

Ｂ３５に格納させる（ステップＳ８）。即ち、図７に示すように、ルータ１４のシリアルナンバー「Ｓ０００００１」及び個体パスワード「ａｂｃ１２３」が格納されるとともに、ウィルスチェックが「オン」設定されてチェック対象プロトコル名「ＰＯＰ３」、「ＳＭＴＰ」、「ＨＴＴＰ」が格納され、さらに、ジャンクメールチェックが「オン」設定されてチェック対象プロトコル名「ＰＯＰ３」が格納される。

【００５７】

このようなセキュリティ契約情報の格納処理が終了すると、契約代行サーバ３４は、契約完了通知をＰＣ１０に送信する（ステップＳ９）。この契約完了通知には、セキュリティサーバ５１のＩＰアドレスと、セキュリティ契約情報に基づくチェック対象プロトコル名及び宛先ポート番号とが含まれている。

【００５８】

ＰＣ１０は上記契約完了通知を受信すると、受信した契約完了通知からセキュリティサーバ５１のＩＰアドレスと、チェック対象プロトコル名及び宛先ポート番号を抽出し、これらをルータ１４に通知する（ステップＳ１０）。

【００５９】

これに応じて、ルータ１４は、通知されたセキュリティサーバ５１のＩＰアドレスをフラッシュメモリ１４４に書き込むとともに、通知されたチェック対象プロトコルと宛先ポート番号とを関連付けたチェック対象プロトコルテーブルをフラッシュメモリ１４４に記憶させる（ステップＳ１１）。

【００６０】

さて、契約代行サーバ３４は、ステップＳ９の処理を行う一方で、セキュリティ契約情報をセキュリティサーバ５１に送信する（ステップＳ１２）。

セキュリティサーバ５１は、このセキュリティ契約情報を受信すると、受信したセキュリティ契約情報をセキュリティ契約情報ＤＢ５３に格納する（ステップＳ１３）。これにより、セキュリティチェックの契約に関する処理が終了することとなる。

【００６１】

（２）ＰＯＰ３を用いた受信メールに対するセキュリティチェック

次に、図１７に示すシーケンスを参照しながら、ＰＯＰ３を用いた受信メールに対してセキュリティチェックを行う際の動作について説明する。

【００６２】

まず、ユーザが例えばＰＣ１０を用いて受信メールの取得を指示する操作を行うと、ＰＣ１０はこの操作を受け付け（ステップＳ２１）、ＰＯＰサーバ３１に対する接続要求をパケットとして送信する（ステップＳ２２）。そして、ルータ１４は、この接続要求を受信する。

【００６３】

ここで、ルータ１４のＣＰＵ１４１は、図１８に示す処理フローが記述されたルーティングプログラムを常時実行している（ステップＳ２３）。

図１８において、ルータ１４のＣＰＵ１４１は、パケットを受信すると（ステップＳ１０１；Ｙｅｓ）、このパケットがチェック対象となるアプリケーション層プロトコルに従うパケットであるか否かを判断する（ステップＳ１０２）。より具体的には、ＣＰＵ１４１は、パケットのＴＣＰヘッダに含まれている宛先ポート番号と、フラッシュメモリ１４４のチェック対象プロトコルテーブル（図３参照）に記述されている宛先ポート番号とが一致する場合にはチェック対象であると判断し、一致しない場合にはチェック対象でないと判断する。ここでは、受信したパケットはＰＯＰ３に基づくものであるので、ＣＰＵ１４１はチェック対象であると判断することになる（ステップＳ１０２；Ｙｅｓ）。

【００６４】

次いで、ＣＰＵ１４１は、ＩＰヘッダに含まれる送信元アドレスがセキュリティサーバ５１のＩＰアドレスであるか否かを判断する（ステップＳ１０３）。

ここで、ＩＰヘッダに含まれている送信元アドレスを参照する理由は、セキュリティサーバ５１から情報通信装置１０～１３宛に送信されたパケットがルータ１４によってセキュリティサーバ５１に返信されてしまうと、情報通信装置１０～１３にパケットが到達しなくなってしまうからである。また、上記理由に加えて、セキュリティサー５１から送信されてきたデータであればコンピュータウィルス等の虞がないものと判断されるという理由もある。

ここでは、パケットの送信元アドレスはＰＣ１０のＩＰアドレスであるので、

セキュリティサーバ５１のＩＰアドレスではないと判断する（ステップＳ１０３；Ｎｏ）。

【００６５】

ステップＳ１０２及びステップＳ１０３における処理によって転送が必要と判断されると、ＣＰＵ１４は、セキュリティサーバ５１と通信コネクションを確立しているか否かを判断する（ステップＳ１０４）。

ここで、通信コネクションが確立されていない場合は（ステップＳ１０４；Ｎｏ）、ＣＰＵ１４は、所定の接続手順に従ってセキュリティサーバ５１との間で通信コネクションを確立する（ステップＳ１０５）。

【００６６】

セキュリティサーバ５１との間で通信コネクションが確立すると、図１１で説明したように、ＣＰＵ１４は、宛先アドレスをセキュリティサーバ５１のＩＰアドレスとし、送信元アドレスを自身のＩＰアドレスとし、さらにルータ１４のシリアルナンバーを含むようにしてカプセル化を行う（ステップＳ１０６）。

【００６７】

そして、ＣＰＵ１４は、カプセル化したパケットをセキュリティサーバ５１に送信する(ステップＳ１０７）。

なお、ステップＳ１０２においてチェック対象プロトコルではないと判断された場合（ステップＳ１０２；Ｎｏ）と、ステップＳ１０３において送信元がセキュリティサーバ５１であると判断された場合（ステップＳ１０３；Ｙｅｓ）には、ＣＰＵ１４１は、パケットをカプセル化することなく、そのままルーティングすることになる。

このように、ルータ１４がパケットを受信するたびに図１８に示すフローが繰り返し実行されることになる。以下では、ルータ１４が外部からパケットを受信する度に上記フローの説明を繰り返すことは省略するが、このフローは、（２）ＰＯＰ３を用いた受信メールに対するセキュリティチェック、だけではなく、（３）ＳＭＴＰを用いた送信メールに対するセキュリティチェック、（４）ＨＴＴＰレスポンスに対するセキュリティチェック、においても同様に実行される。

【００６８】

再び、図１７に戻り、システム全体の動作説明を行う。

図１７のステップＳ２３においては、ルータ１４とセキュリティサーバ５１との間で通信コネクションが確立されていない場合を示している。ステップＳ２４～ステップＳ２６は、図１８のステップＳ１０５で説明した、ルータ１４とセキュリティサーバ５１との間で通信コネクションを確立する処理を示しており、以下簡単に説明する。

まず、ルータ１４は、セキュリティサーバ５１に対しコネクション確立要求を送信する（ステップＳ２４）。このコネクション確立要求には、ルータ１４のシリアルナンバーが含まれている。

【００６９】

セキュリティサーバ５１は接続要求を受信すると、このコネクション確立要求からシリアルナンバーを抽出し、シリアル情報ＤＢ５２に記憶されているシリアルナンバーと照合してルータ１４の正当性を確認する（ステップＳ２５）。以下、この確認処理をルータ認証と呼ぶ。

【００７０】

ルータ１４の正当性が確認されると、セキュリティサーバ５１は、ルータ１４に許可応答を送信し、これによりルータ１４とセキュリティサーバ５１との間で通信コネクションが確立することになる（ステップＳ２６）。

【００７１】

次に、ルータ１４は、図１８のステップＳ１０６で説明したように、ＰＣ１０から受信した接続要求を示すパケットをカプセル化してセキュリティサーバ５１に送信する。これに応じて、セキュリティサーバ５１は、図９で説明したように、ルータ認証を行い、さらに、受信したパケットに対して脱カプセル化を行った後、ＩＰヘッダ内のＩＰアドレスを書き換え、書き換え後の接続要求をＰＯＰサーバ３１に送信する（ステップＳ２７）。

【００７２】

ＰＯＰサーバ３１は、接続要求を受信すると、これに応答して、ＰＣ１０に対し認証情報の送信を要求する認証要求をパケットとして送信する（ステップＳ２８）。この認証要求は、セキュリティサーバ５１及びルータ１４間でトンネリン

グされながら伝送され、ＰＣ１０によって受信される。

【００７３】

そして、ＰＣ１０は、ユーザＩＤやパスワードといった認証情報をメモリから読み出し（ステップＳ２９）、これをＰＯＰサーバ３１に送信する（ステップＳ３０）。この際、これらの認証情報はステップＳ２１の操作受付時にユーザによって入力されていてもよいし、ＰＣ１０の不揮発性メモリから読み出されて自動送信されるような設定が予めなされていてもよい。

この認証情報は、ルータ１４及びセキュリティサーバ５１間でトンネリングやルータ認証が実行されながら伝送され、ＰＯＰサーバ３１によって受信される。

【００７４】

ＰＯＰサーバ３１は認証情報を受信すると、この認証情報からユーザＩＤとパスワードを抽出し、ユーザ情報ＤＢ３５に記憶されているユーザＩＤ及びパスワードと照合してユーザ認証を行う（ステップＳ３１）。

これによりユーザの正当性が確認されると、ＰＯＰサーバ３１は、許可応答を送信する（ステップＳ３２）。この許可応答は、セキュリティサーバ５１及びルータ１４間でトンネリングされながら伝送され、ＰＣ１０によって受信される。

【００７５】

ＰＣ１０は、許可応答を受信すると、受信メールを要求するメール要求をＰＯＰサーバ３１に送信する（ステップＳ３３）。このメール要求は、ルータ１４及びセキュリティサーバ５１間でトンネリングやルータ認証が実行されながら伝送され、ＰＯＰサーバ３１によって受信される。

【００７６】

ＰＯＰサーバ３１はメール要求を受信すると、これに応答して、ユーザＩＤによって特定されるメールボックスから受信メールを示すメールデータを読み出し（ステップＳ３４）、読み出したメールデータをパケットとしてＰＣ１０に送信する（ステップＳ３５）。

【００７７】

一方、セキュリティサーバ５１は、ハードディスク装置５１５に記憶されているセキュリティチェックプログラムを常時実行しており、メールデータを受信す

ると、これに応じて、図６に示すセキュリティ契約情報ＤＢ５３２に記憶されている内容に従い、ウィルスチェック及びジャンクメールチェックを行う（ステップＳ３６）。

ここで、セキュリティサーバ５１によって受信されたデータがセキュリティチェックの対象となるメールデータであるか否かということは、受信したデータが電子メールの書式に従うものであるか否かということにより判断される。

【００７８】

次いで、セキュリティサーバ５１はセキュリティチェックを行った後のメールデータをパケットに分割してカプセル化を行い、ＰＣ１０に送信する（ステップＳ３７）。ルータ１４は、このメールデータを脱カプセル化してＰＣ１０に送信する。

ＰＣ１０は、メールデータを受信すると、ＰＯＰサーバ３１に対して切断要求を送信する（ステップＳ３８）。これによって、ＰＣ１０とＰＯＰサーバ３１との間の通信コネクションが切断され、処理が終了する。

なお、ＩＭＡＰ４を用いた受信メールに対するセキュリティチェックも、上述したＰＯＰ３の場合と同様の動作となる。

【００７９】

（３）ＳＭＴＰを用いた送信メールに対するセキュリティチェック

次に、図１９に示すシーケンスを参照しながら、ＳＭＴＰを用いた送信メールに対してセキュリティチェックを行う際の動作について説明する。

まず、ユーザがＰＣ１０を用いて電子メールの送信を指示する操作を行うと、ＰＣ１０はこの操作を受け付け（ステップＳ５１）、ＳＭＴＰサーバ３３に対する接続要求をパケットとして送信する（ステップＳ５２）。

【００８０】

ルータ１４はこの接続要求を受信すると、図１７のステップＳ２４～Ｓ２６において説明した動作と同様に、セキュリティサーバ５１に対してコネクション確立要求を送信する（ステップＳ５３）。このコネクション確立要求には、ルータ１４のシリアルナンバーが含まれており、セキュリティサーバ５１はこのシリアルナンバーを用いてルータ１４の正当性を確認する（ステップＳ５４）。これに

より正当性が確認されると、セキュリティサーバ５１は、ルータ１４に許可応答を送信し（ステップＳ５５）、これにより通信コネクションが確立することになる。

【００８１】

次に、ルータ１４は、ＰＣ１０から受信した接続要求を示すパケットをカプセル化してセキュリティサーバ５１に送信する。これに応じて、セキュリティサーバ５１は、ルータ認証を行い、さらに、受信したパケットに対して脱カプセル化を行った後、ＩＰアドレスの書き換えを行い、書き換え後の接続要求をＳＭＴＰサーバ３３に送信する（ステップＳ５６）。

【００８２】

ＳＭＴＰサーバ３３は、上記接続要求を受信すると、これに応じて、許可応答を送信する（ステップＳ５７）。この許可応答は、セキュリティサーバ５１及びルータ１４間でトンネリングによって伝送され、ＰＣ１０によって受信される。

【００８３】

ＰＣ１０は、許可応答を受信すると、送信メールを示すメールデータをパケットとしてＳＭＴＰサーバ３３に送信する（ステップＳ５８）。ルータ１４は、ＰＣ１０から受信したメールデータのパケットをカプセル化してセキュリティサーバ５１に送信する。

セキュリティサーバ５１は、このパケットを受信すると、これに応じてルータ認証を行い、さらに、受信したパケットに対して脱カプセル化を行う。そして、セキュリティサーバ５１は、受信したパケットによって構成されるデータがＳＭＴＰに従うメールデータであることを検出すると、セキュリティ契約情報ＤＢ５３に記憶されている内容に従ってウィルスチェックを行う（ステップＳ５９）。

【００８４】

次いで、セキュリティサーバ５１はセキュリティチェックを行った後のメールデータをパケットに分割し、ＩＰアドレスを書き換えてＳＭＴＰサーバ３３に送信する（ステップＳ６０）。

【００８５】

ＳＭＴＰサーバ３３はメールデータを受信すると、ＰＣ１０に対し受信通知を

送信し（ステップＳ６１）、これを受信したＰＣ１０がＳＭＴＰサーバ３３に対し切断要求を送信する（ステップＳ６２）。これによって、ＰＣ１０とＳＭＴＰサーバ３３との間の通信コネクションが切断され、処理が終了する。

【００８６】

（４）ＨＴＴＰを用いたコンテンツデータに対するセキュリティチェック

次に、図２０に示すシーケンスを参照しながら、コンテンツデータに対してセキュリティチェックを行う際の動作について説明する。

まず、ユーザが例えばＰＣ１０を用いてWWWサーバ６のＵＲＬを指定する等してコンテンツの取得を指示する操作を行うと、ＰＣ１０はこの操作を受け付け（ステップＳ７１）、WWWサーバ６に対するＨＴＴＰリクエストをパケットとして送信する（ステップＳ７２）。

【００８７】

ルータ１４のＣＰＵ１４１は、ＨＴＴＰリクエストを受信すると、図１７のステップＳ２４～Ｓ２６において説明した動作と同様に、セキュリティサーバ５１に対してコネクション確立要求を送信する（ステップＳ７３）。このコネクション確立要求には、ルータ１４のシリアルナンバーが含まれており、セキュリティサーバ５１はこのシリアルナンバーを用いてルータ１４の正当性を確認する（ステップＳ７４）。これによりルータ１４の正当性が確認されると、セキュリティサーバ５１は、ルータ１４に許可応答を送信し（ステップＳ７５）、これにより通信コネクションが確立することになる。

【００８８】

次に、ルータ１４は、ＰＣ１０から受信したＨＴＴＰリクエストをカプセル化してセキュリティサーバ５１に送信する（ステップＳ７６）。

【００８９】

セキュリティサーバ５１は、受信したパケットに対し脱カプセル化を行った後、ＩＰヘッダのＩＰアドレスを書き換えてWWWサーバ６に送信する（ステップＳ７７）。

【００９０】

WWWサーバ６は、ＨＴＴＰリクエストを受信すると、これに応答して、ＨＴ

ＴＰリクエストに含まれるＵＲＬによって指定されるリソースからコンテンツデータを読み出し（ステップＳ７８）、読み出したコンテンツデータをＨＴＴＰレスポンスとしてＰＣ１０に送信する（ステップＳ７９）。

【００９１】

セキュリティサーバ５１はこのコンテンツデータを受信すると、セキュリティ契約情報ＤＢ５３に記憶されている内容に従ってウィルスチェックを行う（ステップＳ８０）。

次いで、セキュリティサーバ５１は、セキュリティチェックを行った後のコンテンツデータをパケットに分割し、ＩＰアドレスを書き換えてＰＣ１０に送信する。ルータ１４は、このＨＴＴＰレスポンスを脱カプセル化してＰＣ１０に送信し、ＰＣ１０はこれを受信する（ステップＳ８１）。そして、ＰＣ１０は、受信したコンテンツデータを解釈してこれを表示する。

【００９２】

上述した実施形態によれば、ルータ１４が受信したデータがＰＯＰ３、ＩＭＡＰ４及びＨＴＴＰに従うデータである場合、ルータ１４が上記データをセキュリティサーバ５１に転送すると、セキュリティサーバ５１は、受信したデータを当該データの宛先であるＰＯＰサーバ３１、ＩＭＡＰサーバ３２又はWWWサーバ６へ送信し、これに応答してＰＯＰサーバ３１、ＩＭＡＰサーバ３２又はWWWサーバ６から送信されてくるデータに対してセキュリティチェックを行うので、コンピュータウィルス等の様々な不正行為による被害を防止することができる。

【００９３】

また、ルータ１４が受信したデータがＳＭＴＰに従うデータである場合、ルータ１４が受信したデータをセキュリティサーバ５１に転送すると、これに応じて、セキュリティサーバ５１が、ルータ１４から転送されてきたデータに対してセキュリティチェックを行うので、コンピュータウィルス等の様々な不正行為による被害を防止することができる。

【００９４】

さらに、上記のセキュリティチェックを行う場合、ユーザが所有する情報通信装置１０～１３側ではなく、セキュリティサーバ５１側でセキュリティチェック

を行うので、ユーザがワクチンソフトをアップデートするというような作業が不要となる。これによりユーザの利便性を向上させることができる。

【００９５】

さらに、ルータ１４のシリアルナンバーを用いてルータ認証を行うので、セキュリティサーバ５１は、不正なルータによるアクセスを排除することができる。

【００９６】

さらに、セキュリティチェックの契約や課金に関する処理は、本来の処理主体であるべきセンタ５に代わってＩＳＰ３が行うので、センタ５の管理者としては上記処理を行うための新たなシステムを開発する必要がない。また、ＩＳＰ３側も、自身の既存システムに大きな変更を加えることなく、上記処理を実行できるので便利である。

【００９７】

Ｃ：変形例

既述の通り、本発明は上述した実施形態に限定されず、以下のような種々の変更が可能である。

【００９８】

（１）ルータ１４の形態

実施形態では、セキュリティサーバ５１に対してデータを転送する装置としてルータ１４を例示した。しかし、必ずしもこれに限定されるわけではなく、要は、情報通信装置１０～１３宛のデータや情報通信装置１０～１３から送信されるデータが伝送される伝送路に配置されて、上記データを中継するデータ中継装置であればよい。このようなデータ中継装置は、通常、その装置がサポートするプロトコル層に応じて、リピータ、ブリッジ、ルータ或いはゲートウェイというように異なる呼び方で呼ばれているが、実施形態で述べた構成及び動作を備えたデータ中継装置であれば、その呼び方に限定されることなく、本発明の技術思想に含まれる。

また、ルータ１４はホームネットワーク１に利用されるだけでなく、例えばオフィス内に設置された社内ＬＡＮ（Local Area Network）のような様々なローカルネットワークに利用可能である。

なお、ルータ１４に接続される情報通信装置１０～１３は図１に示す４台に限定されず、もっと多くても少なくてもよいことはもちろんである。

【００９９】

（２）ルータ認証に用いる情報

実施形態では、ルータ認証を行う際に、そのルータ１４の製造時に割り当てられたシリアルナンバーを用いていた。このシリアルナンバーは、ルータ１４のハードウェアに対するシリアルナンバーであってもよいし、ルータ１４に搭載されるルーティングプログラム等のソフトウェアに対するシリアルナンバーであってもよい。

また、ルータ認証に用いられる情報は、必ずしもシリアルナンバーに限定されるわけではない。要は、各ルータ１４を識別できる情報であればよく、例えば、ルータ１４に割り当てられたＭＡＣアドレス等を代用してもよい。

また、ルータ１４によって転送されるパケットに対してシリアルナンバーを記述する場合、その記述エリアは、カプセル化によって付加されたＴＣＰペイロードに限定されるわけではなく、例えば、カプセル化によって付加されたＩＰヘッダやＴＣＰヘッダ等の適当なフィールドを利用すればよい。

【０１００】

（３）セキュリティチェックの対象となるプロトコル

実施形態では、ＰＯＰ３、ＩＭＡＰ４、ＳＭＴＰ、ＨＴＴＰというプロトコルを例に挙げてセキュリティチェックを行うようにしていたが、必ずしもこれに限らず、例えばＦＴＰ（File Transfer Protocol）に従うデータに対してセキュリティチェックを行うようにしてもよい。

また、ルータ１４が記憶しているチェック対象プロトコルテーブルには、チェック対象となるプロトコルが記述されていたが、これとは逆に、チェック対象ではないプロトコルを記述しておき、ルータ１４はこのチェック対象プロトコルテーブルに記述されていないプロトコルに従うデータを受信した場合に当該データをセキュリティサーバ５１に転送するようにしてもよい。

【０１０１】

（４）ネットワーク構成

実施形態では、ホームネットワーク１とＩＳＰ３との間に介在するネットワークとしてＡＤＳＬ網２を例示したが、これに限定されない。このネットワークの周波数帯域は広帯域であっても狭帯域であってもよく、例えば公衆電話網、ＩＳＤＮ（Integrated Service Digital NetWork）網、ＣＡＴＶ（Cable TV）網、いわゆる×ＤＳＬ網、携帯電話網等の公衆無線ネットワーク、衛星通信ネットワーク等の様々なネットワークが利用できる。

なお、このように図１とネットワーク形態が異なる場合には、ＡＤＳＬモデム１５に代えて、そのネットワークに適した変復調装置やプロトコル変換装置を用いる必要がある。

【０１０２】

（５）ＨＴＴＰリクエストに対するセキュリティチェック

実施形態では、図２０において説明したように、ＨＴＴＰレスポンスとしてのコンテンツデータに対してセキュリティチェックを行うようになっていたが、ＨＴＴＰリクエストに対してセキュリティチェックを行ってもよい。即ち、最近では、閲覧者に対し不適切なコンテンツを提供するサイトの存在も問題視されており、上述したＨＴＴＰリクエストに対するセキュリティチェックは、このようなサイトへのＨＴＴＰリクエストを排除することを目的としたものである。

具体的には、セキュリティサーバ５１が、例えば成人向けのコンテンツを提供するサイトのＵＲＬを蓄積しておき、ＰＣ１０からのＨＴＴＰリクエストを中継する際にはそのＨＴＴＰリクエストに含まれるＵＲＬと、自身が蓄積しているＵＲＬとを照合し、一致した場合には、そのＨＴＴＰリクエストを廃棄すればよい。このようなセキュリティチェックをＵＲＬフィルタリングと呼ぶことにする。このＵＲＬフィルタリングを行うタイミングは、図２０のステップＳ７６とステップＳ７７の間となる。

【０１０３】

（６）セキュリティチェック後の動作

実施形態において、セキュリティチェックサーバ５１がセキュリティチェックを行ってコンピュータウィルスを駆除したり、ジャンクメールを廃棄したりした場合には、その旨を情報通信装置１０～１３に通知するようにすればさらに望ま

しい。

【０１０４】

（７）セキュリティ契約情報の配信

実施形態では、契約代行サーバ３４がチェック対象プロトコル名と宛先ポート番号をＰＣ１０に送信すると、ＰＣ１０がこれらをルータ１４に転送するようになっていた。しかしこれに限定されず、契約代行サーバ３４が直接、ルータ１４に送信するようにしてもよい。

また、図１５のステップＳ６において、契約時にＰＣ１０が送信したデータをルータ１４が中継する際に、そのデータからチェック対象プロトコル名を抽出して、このチェック対象プロトコルに対応する宛先ポート番号と関連付けて記憶するようにしてもよい。

このようにすれば、処理のステップ数が削減されることになる。

【０１０５】

（８）プッシュ型配信への適用

実施形態では、情報通信装置１０～１３からのリクエストに応答してサーバから送信されてくる受信メールやコンテンツ、或いは、情報通信装置１０～１３から送信される送信メールに対してセキュリティチェックを行っていた。

しかしこれに限らず、インターネット４に接続されたサーバから情報通信装置１０～１３に強制的に配信してくるような場合（これをプッシュ型配信と呼ぶ）であっても本発明を適用することが可能である。この場合、ルータ１４は、上記サーバから送信されてくる情報通信装置１０～１３宛のデータを受信すると、これをセキュリティサーバ５１に転送する。一方、セキュリティサーバは、転送されてきたデータに対してセキュリティチェックを行った後に、そのデータの宛先である情報通信装置１０～１３に送信すればよい。

【０１０６】

（９）プログラムの形態

ルータ１４やセキュリティサーバ５１が上述した処理を行うために実行するプログラム（即ち、ルーティングプログラム、セキュリティチェックプログラム、契約申込画面配信プログラム及びプロキシプログラム）は、これらルータ１４や

セキュリティサーバ５１にアプリケーションプログラムとしてインストールされてもよいことはもちろんである。例えば、ルータ１４、セキュリティサーバ５１のＣＰＵ１４１、５１１を用いて読み取り可能な磁気記録媒体、光記録媒体あるいはＲＯＭなどの記録媒体に記録してこのプログラムを提供することができる。

また、このようなプログラムをインターネット４のようなネットワーク経由でルータ１４やセキュリティサーバ５１にダウンロードさせることももちろん可能である。

なお、製造後のルータ１４にルーティングプログラムをインストールする際には、このルーティングプログラムは、ＲＯＭ１４２ではなく、フラッシュメモリ１４４に記憶されることになる。

【０１０７】

【発明の効果】

上述したように本発明によれば、データ中継装置によって転送されてくるデータを当該データの宛先へ送信し、この送信したデータに応答して宛先から送信されてくる応答データを受信すると、この受信した応答データに対してセキュリティチェックを行うので、コンピュータウィルス等の様々な不正行為による被害を防止することができる。

【０１０８】

また、本発明によれば、データ中継装置によって転送されてくるデータを受信すると、受信したデータに対してセキュリティチェックを行うので、コンピュータウィルス等の様々な不正行為による被害を防止することができる。

【０１０９】

【図面の簡単な説明】

【図１】　本発明の実施形態に係るシステム全体の構成を示すブロック図である。

【図２】　実施形態におけるルータの構成を示すブロック図である。

【図３】　実施形態におけるチェック対象プロトコルテーブルに記述されているデータの一例を示すフォーマット図である。

【図４】　実施形態におけるセキュリティサーバの構成を示すブロック図で

ある。

【図５】　実施形態におけるシリアル情報ＤＢに記憶されているシリアル情報の一例を示すフォーマット図である。

【図６】　実施形態におけるセキュリティ契約情報ＤＢに記憶されているセキュリティ契約情報の一例を示すフォーマット図である。

【図７】　実施形態におけるユーザ情報ＤＢに記憶されているユーザ情報の一例を示すフォーマット図である。

【図８】　実施形態における課金情報ＤＢに記憶されている課金情報の一例を示すフォーマット図である。

【図９】　実施形態におけるデータ中継の仕組みを説明する説明図である。

【図１０】　実施形態におけるデータ中継の際のパケットの構造を示す説明図である。

【図１１】　実施形態におけるデータ中継の際のパケットの構造を示す説明図である。

【図１２】　実施形態におけるデータ中継の際のパケットの構造を示す説明図である。

【図１３】　実施形態におけるデータ中継の際のパケットの構造を示す説明図である。

【図１４】　実施形態におけるデータ中継の際のパケットの構造を示す説明図である。
である。

【図１５】　実施形態において契約申込みを行う際のシステム全体の動作を示すシーケンス図である。

【図１６】　実施形態における契約申込画面の一例を示す模式図である。

【図１７】　実施形態において受信メールに対してセキュリティチェックを行う際のシステム全体の動作を示すシーケンス図である。

【図１８】　実施形態におけるルータのＣＰＵがセキュリティチェックプログラムを実行する際のフローチャートである。

【図１９】　実施形態において送信メールに対してセキュリティチェックを

行う際のシステム全体の動作を示すシーケンス図である。

【図２０】　実施形態においてコンテンツデータに対してセキュリティチェックを行う際のシステム全体の動作を示すシーケンス図である。

【符号の説明】

１・・・ホームネットワーク、２・・・ＡＤＳＬ網、

３・・・ＩＳＰ（プロバイダ）、３１・・・ＰＯＰサーバ（宛先）、

３２・・・ＩＭＡＰサーバ（宛先）、３３・・・ＳＭＴＰサーバ（宛先）、

３４・・・契約代行サーバ（プロバイダの通信装置）、

３５・・・ユーザ情報ＤＢ（記憶手段）、３６・・・課金情報ＤＢ（課金手段）、

４・・・インターネット、５・・・センタ、

５１・・・セキュリティサーバ（サーバ、転送先）、

５１１・・・ＣＰＵ（データ受信手段、データ送信手段、応答データ受信手段、セキュリティチェック手段、応答データ送信手段、認証手段）、

５１２・・・ＲＯＭ、５１３・・・ＲＡＭ、

５１４・・・通信部（データ受信手段、データ送信手段、応答データ受信手段、応答データ送信手段）、

５１５・・・ハードディスク装置、５２・・・セキュリティ契約情報ＤＢ、

５３・・・シリアル情報ＤＢ（記憶手段）、６・・・WWWサーバ（宛先）、

７・・・金融機関システム、１０・・・ＰＣ（情報通信装置）、

１１・・・テレビジョン（情報通信装置）、

１２・・・ＭＰ３プレーヤ（情報通信装置）、

１３・・・ＰＤＡ（情報通信装置）、１４・・・ルータ（データ中継装置）、

１４１・・・ＣＰＵ（転送手段、通信手段、判断手段、アドレス受信手段、決定手段、要否判断情報受信手段）、

１４２・・・ＲＯＭ（記憶手段）、１４３・・・ＲＡＭ、

１４４・・・フラッシュメモリ（アドレス記憶手段、要否判断情報記憶手段）、

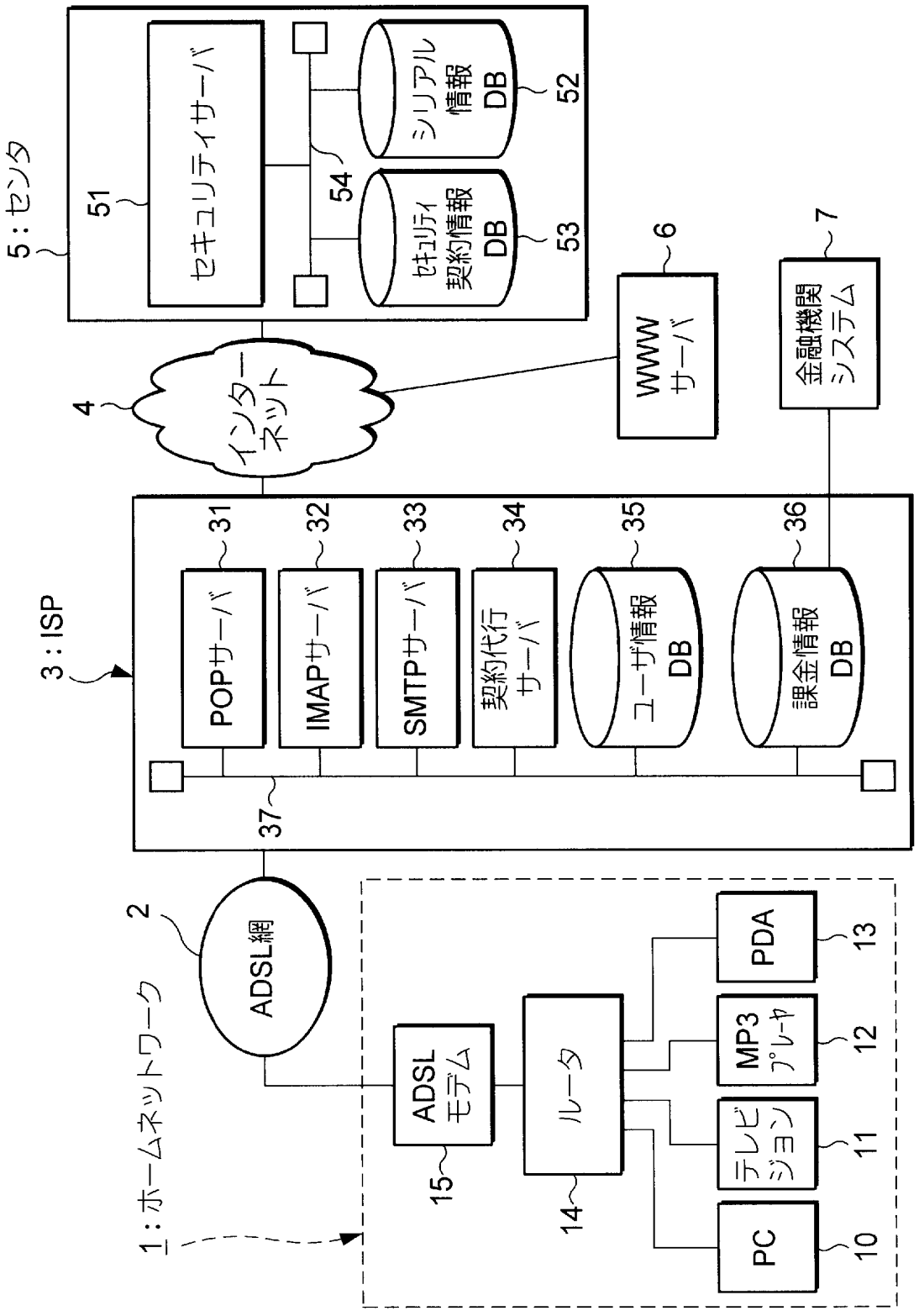
１４５・・・表示部、１４６・・・ＬＡＮ通信部（通信手段）、

１４７・・・ＷＡＮ通信部（通信手段、転送手段、アドレス受信手段、要否判断

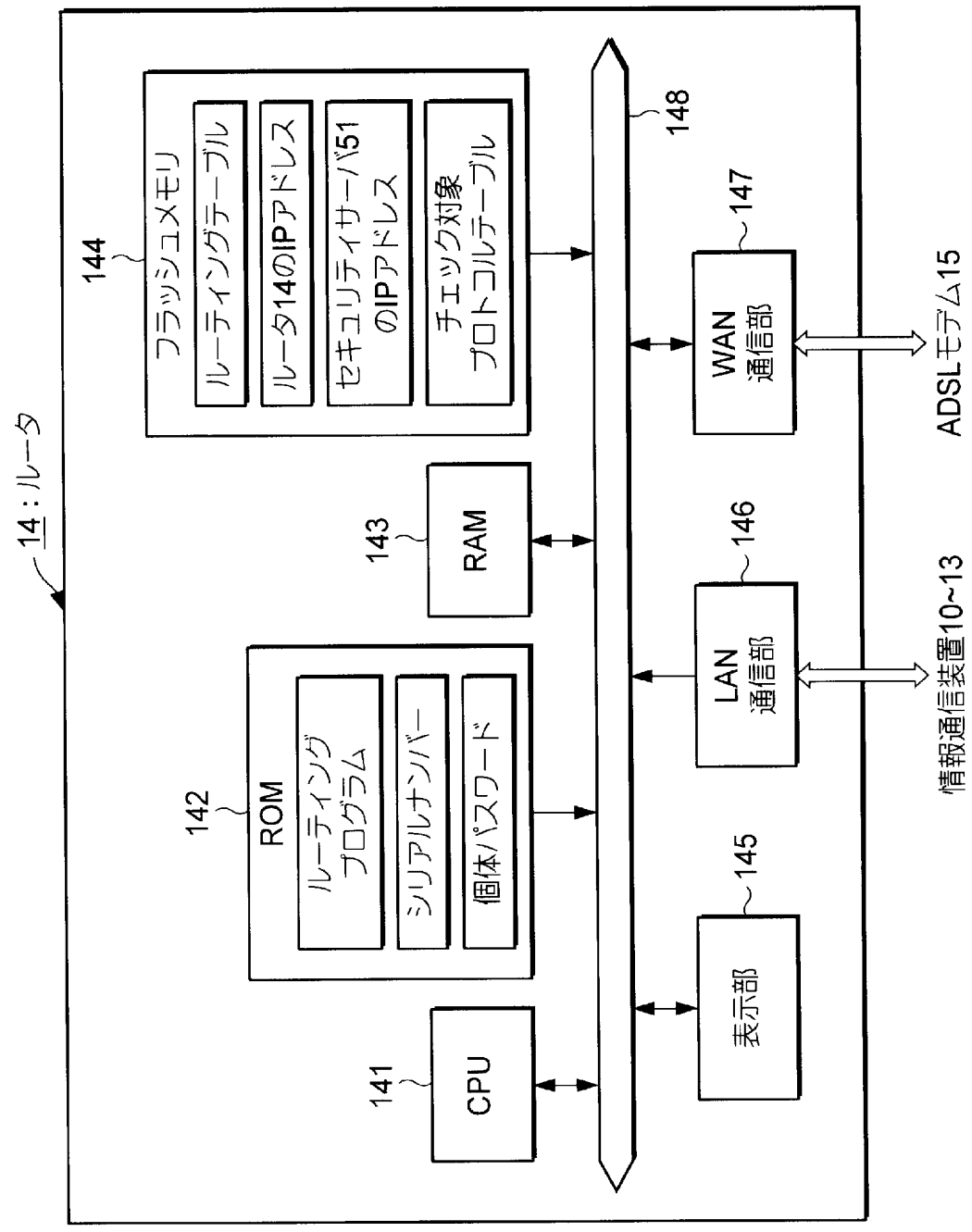
情報受信手段）、１５・・・ＡＤＳＬモデム。

【書類名】　　図面

【図１】


1：ホームネットワーク
2
ADSL網
ADSL
モデム
15
ルータ
14
PC
10
テレビ
ジョン
11
MP3
プレーヤ
12
PDA
13
3：ISP
POPサーバ
31
IMAPサーバ
32
SMTPサーバ
33
契約代行
サーバ
34
ユーザ情報
DB
35
課金情報
DB
36
37
4
インター
ネット
WWW
サーバ
6
金融機関
システム
7
5：センタ
セキュリティサーバ
51
54
シリアル
情報
DB
52
セキュリティ
契約情報
DB
53

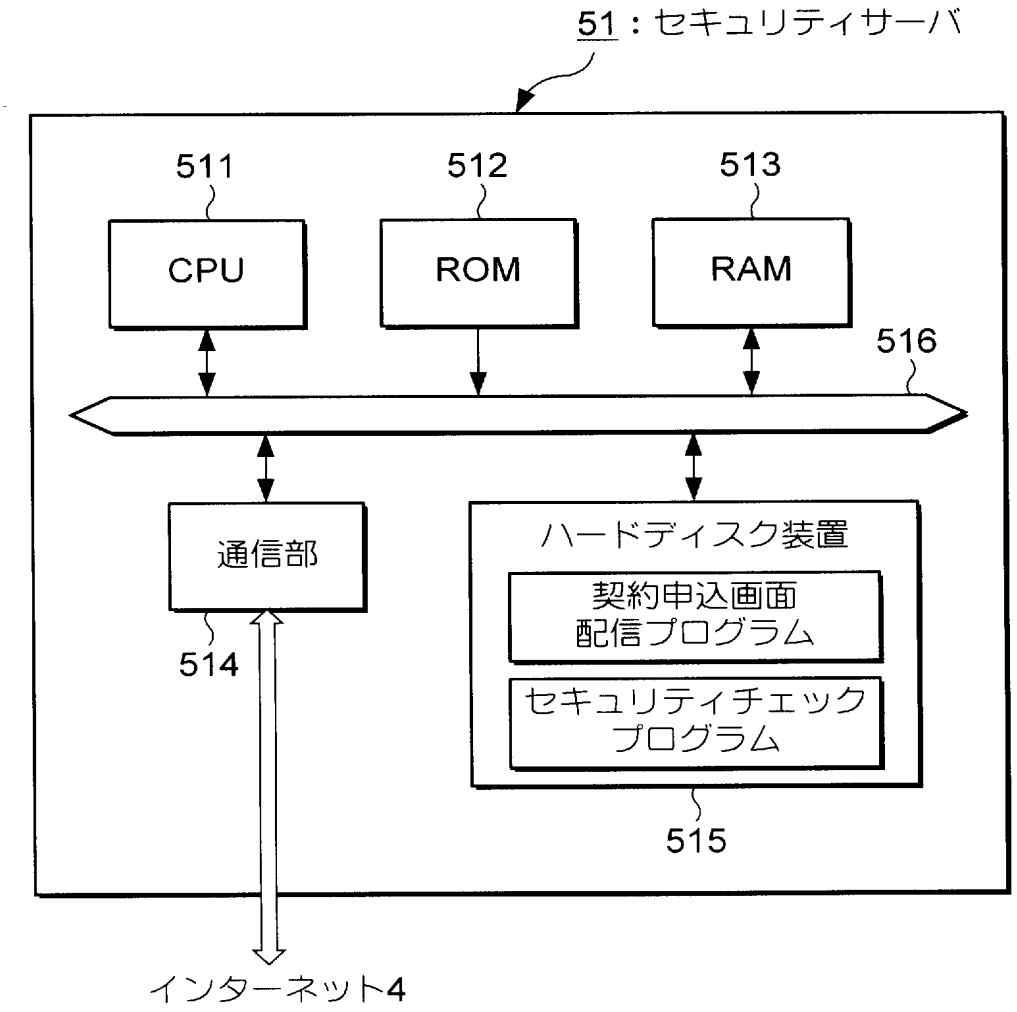
【図２】


14：ルータ
144
フラッシュメモリ
ルーティングテーブル
ルータ14のIPアドレス
セキュリティサーバ51のIPアドレス
チェック対象プロトコルテーブル
148
147
WAN通信部
ADSLモデム15
143
RAM
146
LAN通信部
情報通信装置10~13
142
ROM
ルーティングプログラム
シリアルナンバー
個体パスワード
145
表示部
141
CPU

【図３】

チェック対象プロトコル	宛先ポート番号
POP3	110
SMTP	25
HTTP	80

【図４】



【図５】

シリアルナンバー	個体パスワード
S000001	abc123
S000002	syt254
S000003	ztc921
⋮	⋮
S018110	hfn377

【図６】

シリアルナンバー		S000001	S000002	・・・・・・
セキュリティチェックの内容				
	ウィルスチェック	オン	オフ	・・・・・・
	チェック対象プロトコル	POP3	—	・・・・・・
		SMTP	—	・・・・・・
		HTTP	—	・・・・・・
		—	—	・・・・・・
	ジャンクメールチェック	オン	オン	・・・・・・
	チェック対象プロトコル	POP3	IMAP4	・・・・・・
		—	—	・・・・・・

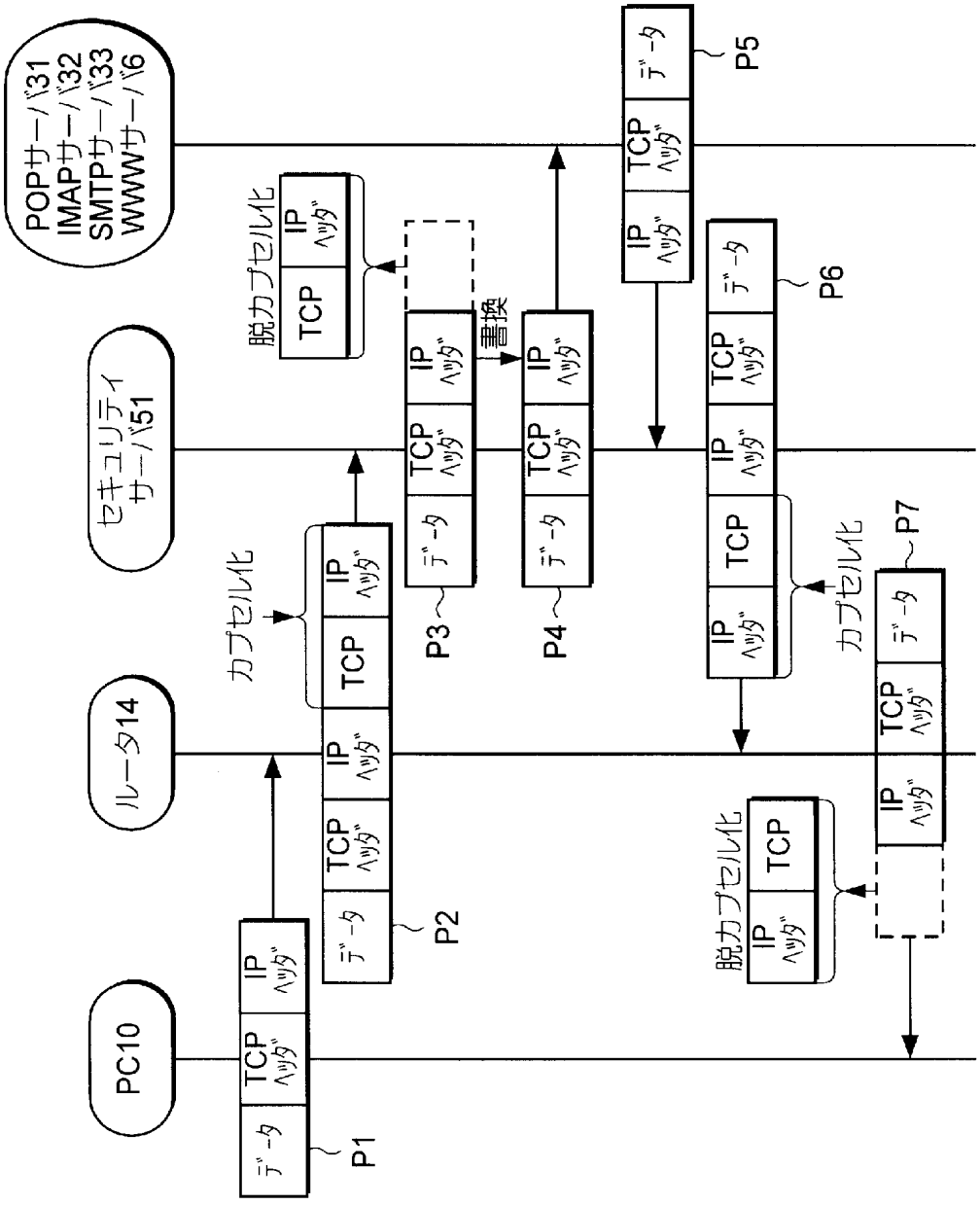
【図７】

ユーザーID	aaa	bbb	・・・・・・・
パスワード	xxxzzz	kkkttt	・・・・・・・
シリアルナンバー	S000001	—	・・・・・・・
個体パスワード	abc123	—	・・・・・・・
セキュリティチェックの内容			
ウィルスチェック	オン	—	・・・・・・・
チェック対象プロトコル	POP3	—	・・・・・・・
	SMTP	—	・・・・・・・
	HTTP	—	・・・・・・・
	—	—	・・・・・・・
ジャンクメールチェック	オン	—	・・・・・・・
チェック対象プロトコル	POP3	—	・・・・・・・
	—	—	・・・・・・・
ユーザ名前	・・・	・・・	・・・・・・・
住　所	・・・	・・・	・・・・・・・
生年月日	・・・	・・・	・・・・・・・
・・・	・・・	・・・	・・・

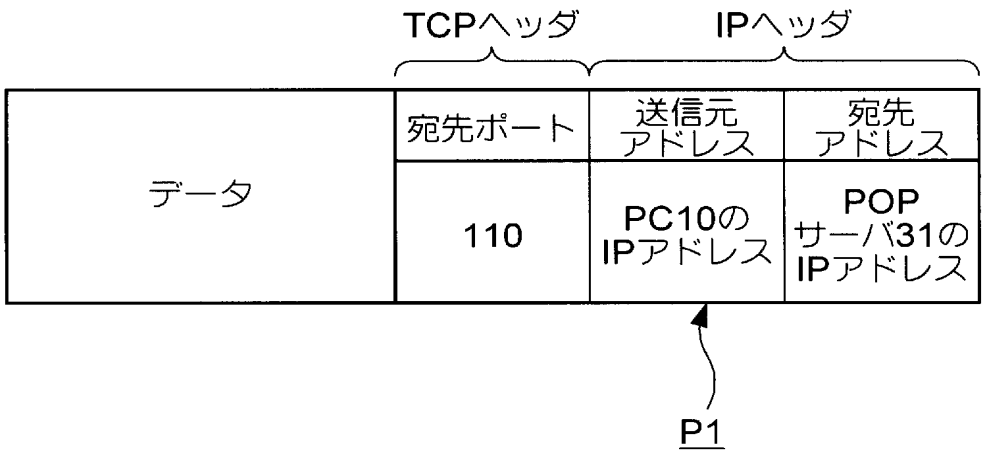
【図８】

ユーザID	aaa	bbb	・・・・・・
銀行口座	○○銀行 △△支店 □座番号:XXXXXXX	××銀行 □□支店 □座番号:XXXXXXX	・・・・・・
ISP課金額	5000	3000	・・・・・・
セキュリティチェック課金額	3000	—	・・・・・・
ウィルスチェック課金額	2000	—	・・・・・・
ジャンクメールチェック課金額	1000	—	・・・・・・
課金額合計	8000	3000	・・・・・・

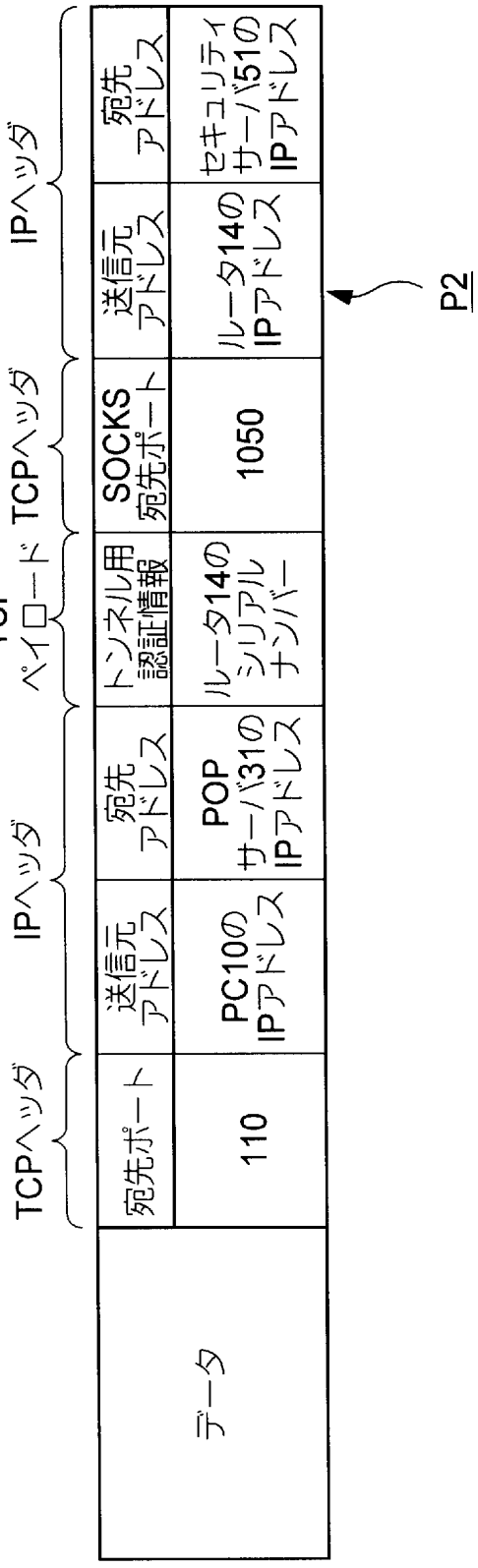
【図９】


POPサーバ31
IMAPサーバ32
SMTPサーバ33
WWWサーバ6
セキュリティサーバ51
ルータ14
PC10
脱カプセル化
カプセル化
書換
データ
TCP ヘッダ
IP ヘッダ
P1
P2
P3
P4
P5
P6
P7

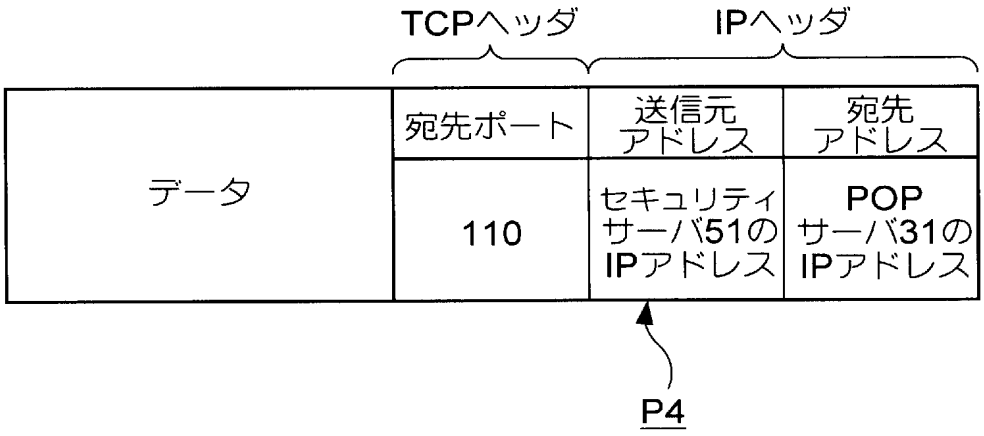
【図１０】


TCPヘッダ
IPヘッダ
データ
宛先ポート
送信元アドレス
宛先アドレス
110
PC10のIPアドレス
POPサーバ31のIPアドレス
P1

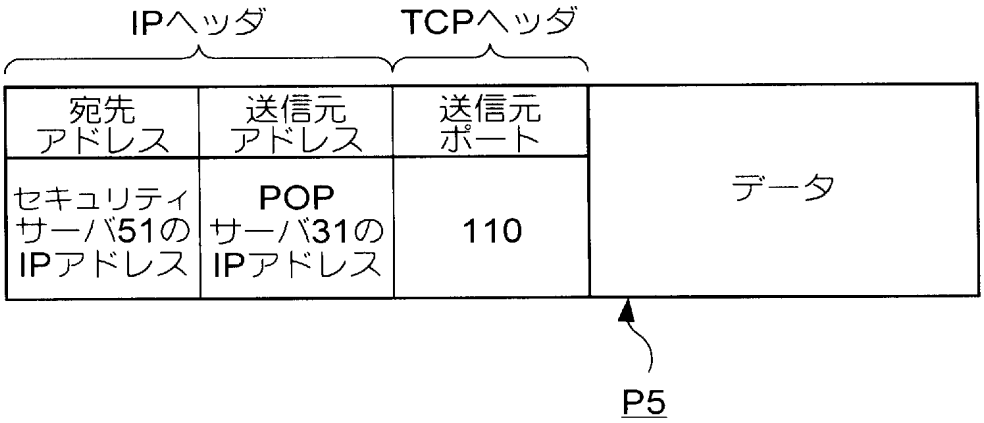
【図１１】


TCPヘッダ
IPヘッダ
TCP
ペイロード
TCPヘッダ
IPヘッダ
データ
宛先ポート
送信元アドレス
宛先アドレス
トンネル用認証情報
SOCKS宛先ポート
送信元アドレス
宛先アドレス
110
PC10のIPアドレス
POPサーバ31のIPアドレス
ルータ14のシリアルナンバー
1050
ルータ14のIPアドレス
セキュリティサーバ51のIPアドレス
P2

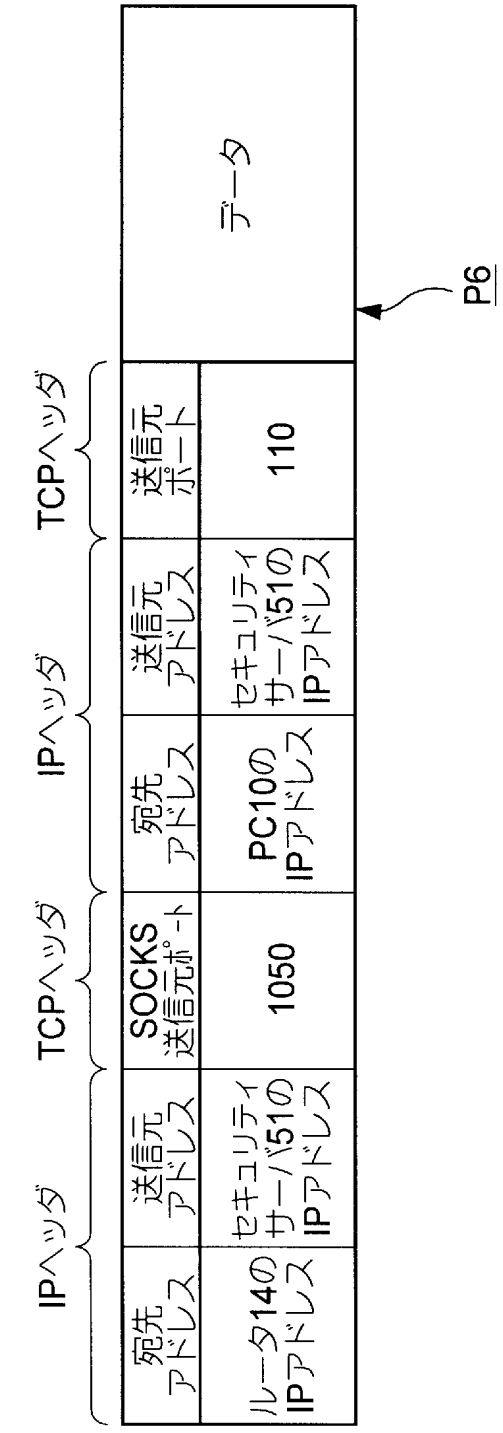
【図１２】


TCPヘッダ
IPヘッダ
データ
宛先ポート
送信元アドレス
宛先アドレス
110
セキュリティサーバ51のIPアドレス
POPサーバ31のIPアドレス
P4

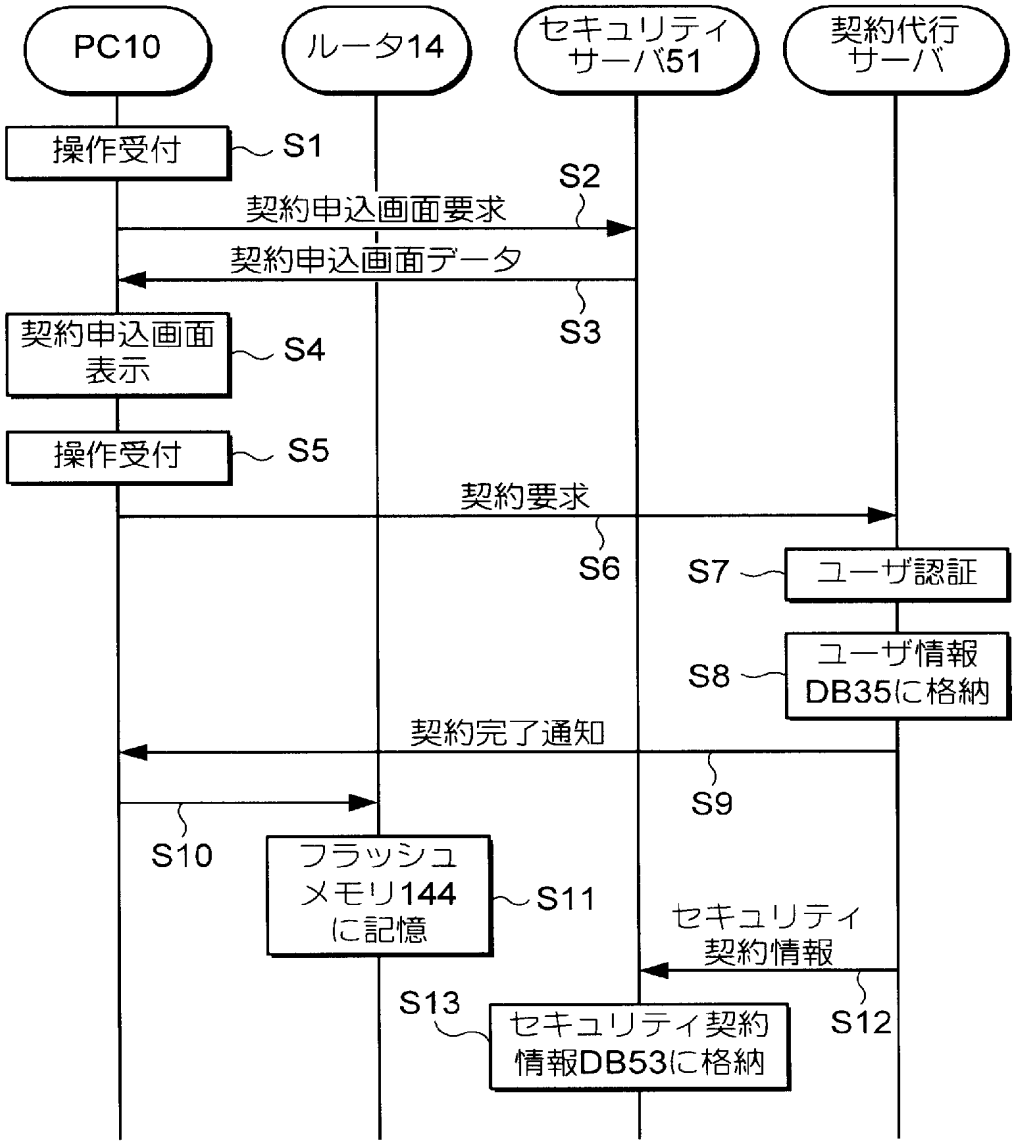
【図１３】


IPヘッダ
TCPヘッダ
宛先アドレス
送信元アドレス
送信元ポート
データ
セキュリティサーバ51のIPアドレス
POPサーバ31のIPアドレス
110
P5

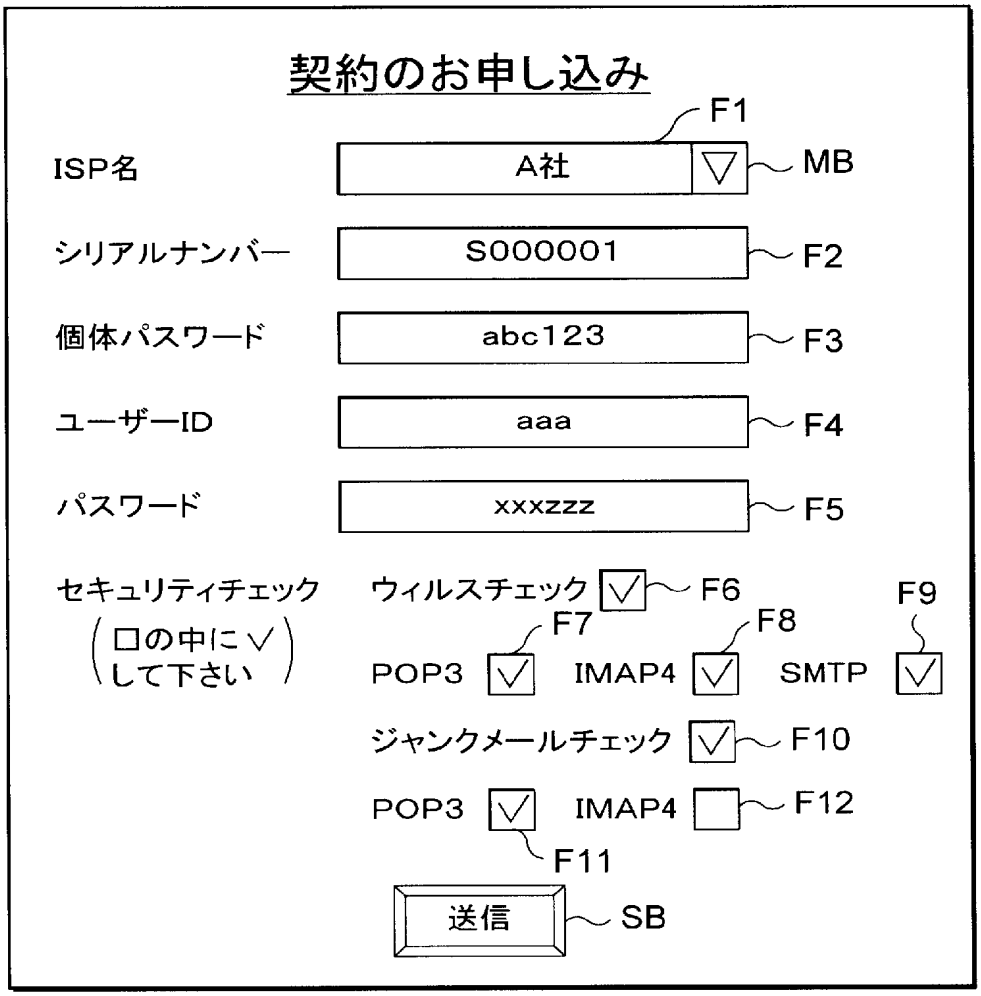
【図１４】


IPヘッダ
TCPヘッダ
IPヘッダ
TCPヘッダ
宛先アドレス
送信元アドレス
SOCKS送信元ポート
宛先アドレス
送信元アドレス
送信元ポート
ルータ14のIPアドレス
セキュリティサーバ51のIPアドレス
1050
PC10のIPアドレス
セキュリティサーバ51のIPアドレス
110
データ
P6

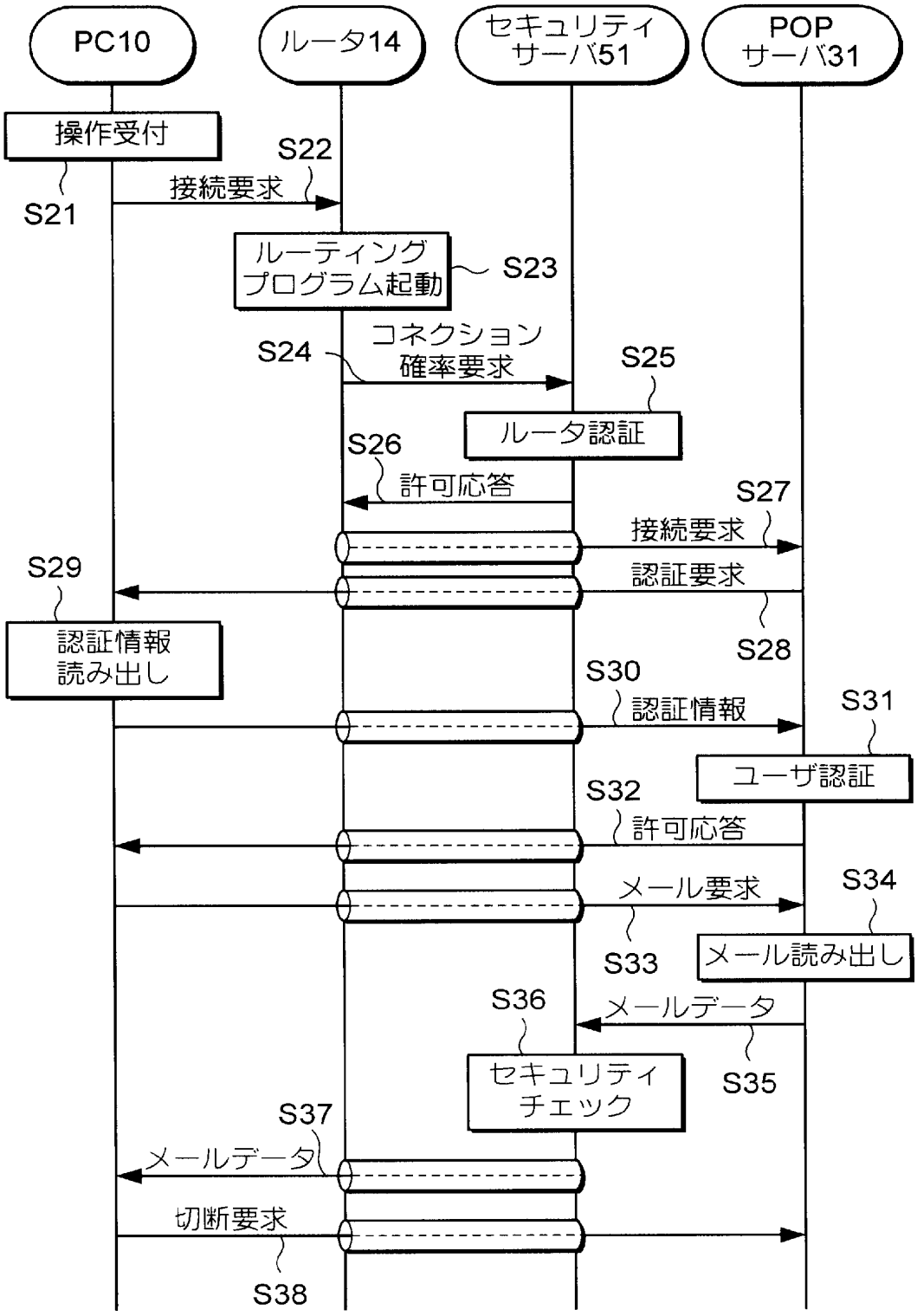
【図１５】


PC10
ルータ14
セキュリティサーバ51
契約代行サーバ
操作受付
S1
S2
契約申込画面要求
契約申込画面データ
S3
契約申込画面表示
S4
操作受付
S5
契約要求
S6
S7
ユーザ認証
S8
ユーザ情報DB35に格納
契約完了通知
S9
S10
フラッシュメモリ144に記憶
S11
セキュリティ契約情報
S12
S13
セキュリティ契約情報DB53に格納

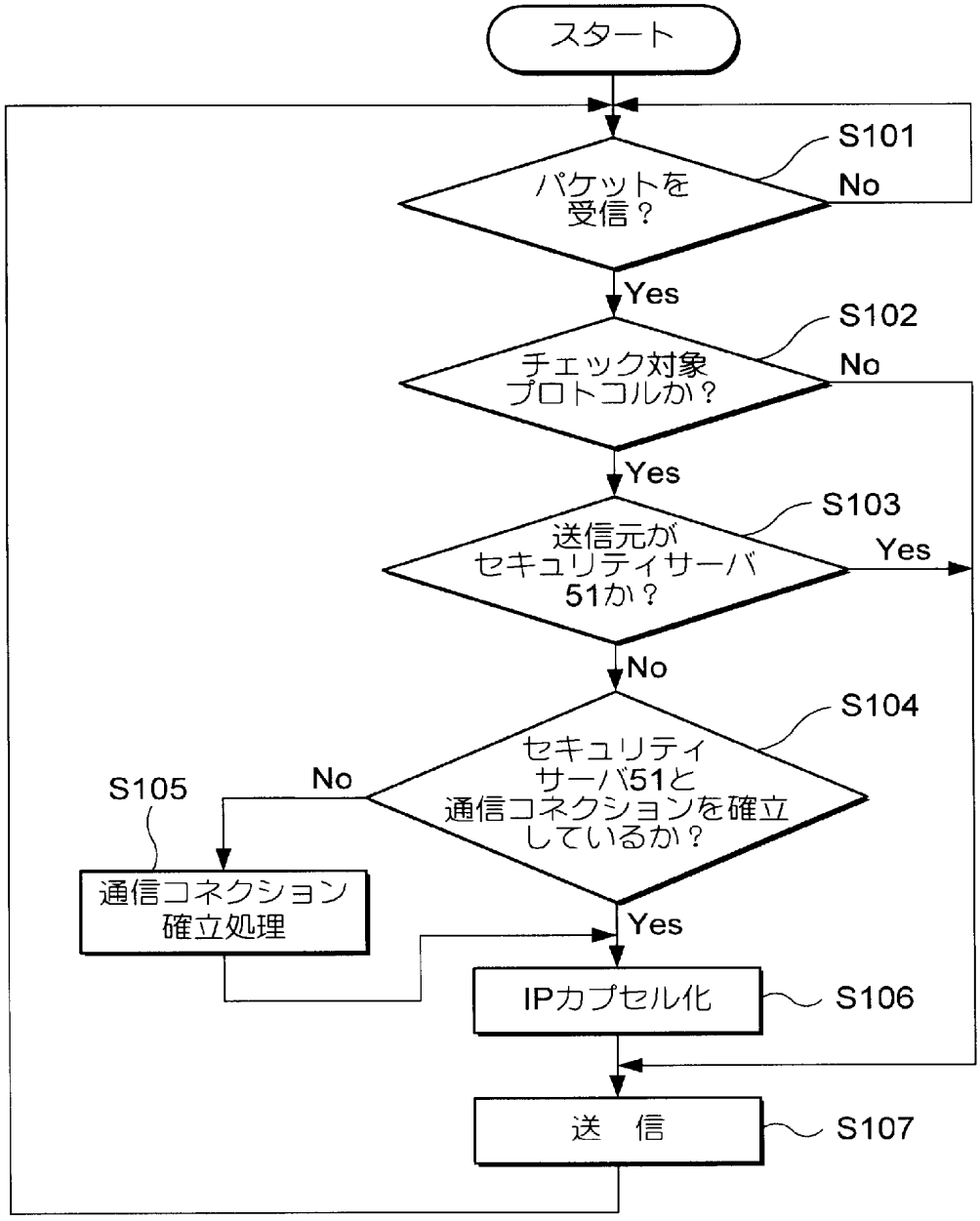
【図１６】


契約のお申し込み
F1
ISP名
A社
MB
シリアルナンバー
S000001
F2
個体パスワード
abc123
F3
ユーザーID
aaa
F4
パスワード
xxxzzz
F5
セキュリティチェック
（□の中に∨して下さい）
ウィルスチェック
F6
F9
F7
F8
POP3
IMAP4
SMTP
ジャンクメールチェック
F10
POP3
IMAP4
F12
F11
送信
SB

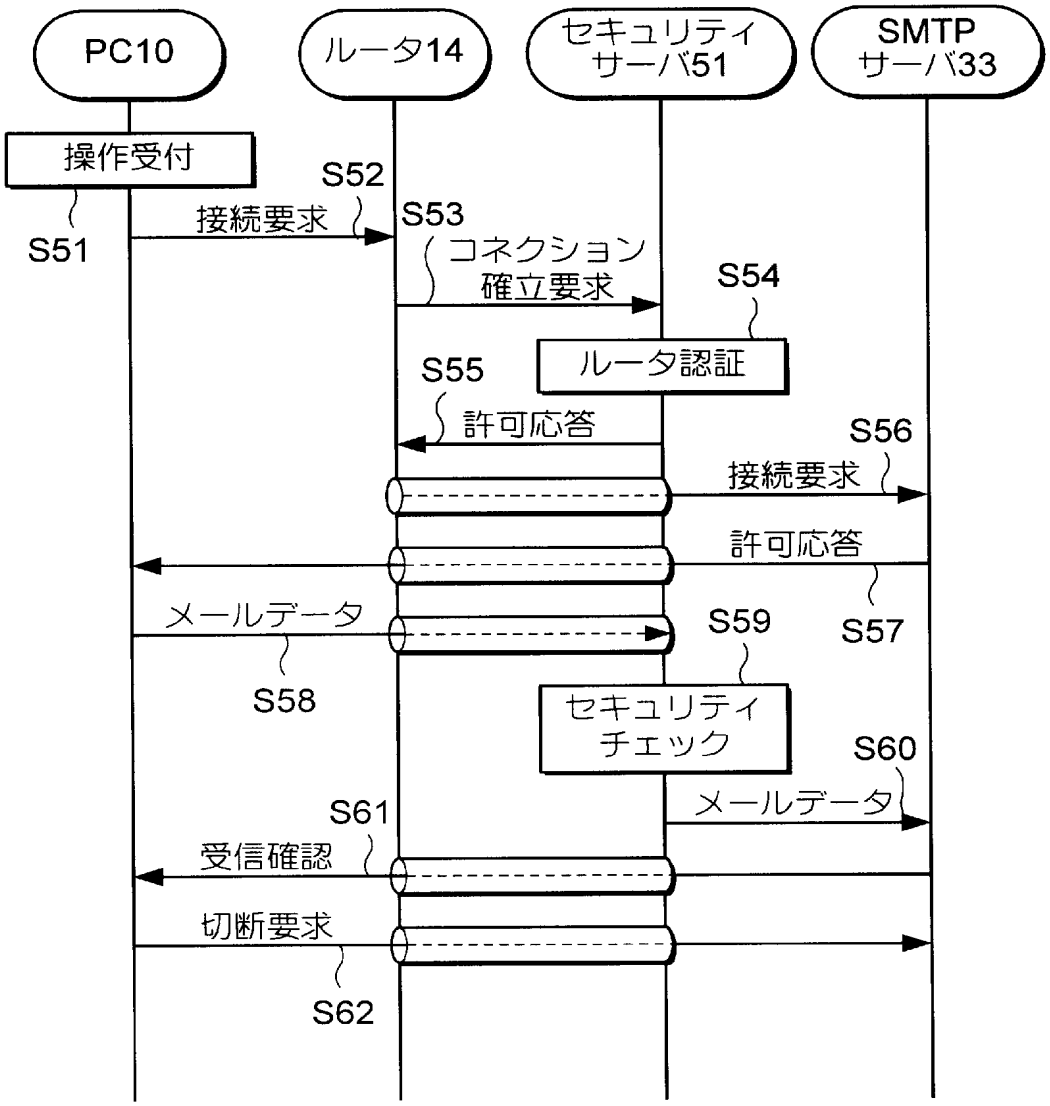
【図１７】


PC10
ルータ14
セキュリティサーバ51
POPサーバ31
操作受付
S21
S22
接続要求
ルーティングプログラム起動
S23
S24
コネクション確率要求
S25
ルータ認証
S26
許可応答
S27
接続要求
S29
認証要求
認証情報読み出し
S28
S30
認証情報
S31
ユーザ認証
S32
許可応答
メール要求
S34
S33
メール読み出し
S36
メールデータ
S35
セキュリティチェック
S37
メールデータ
切断要求
S38

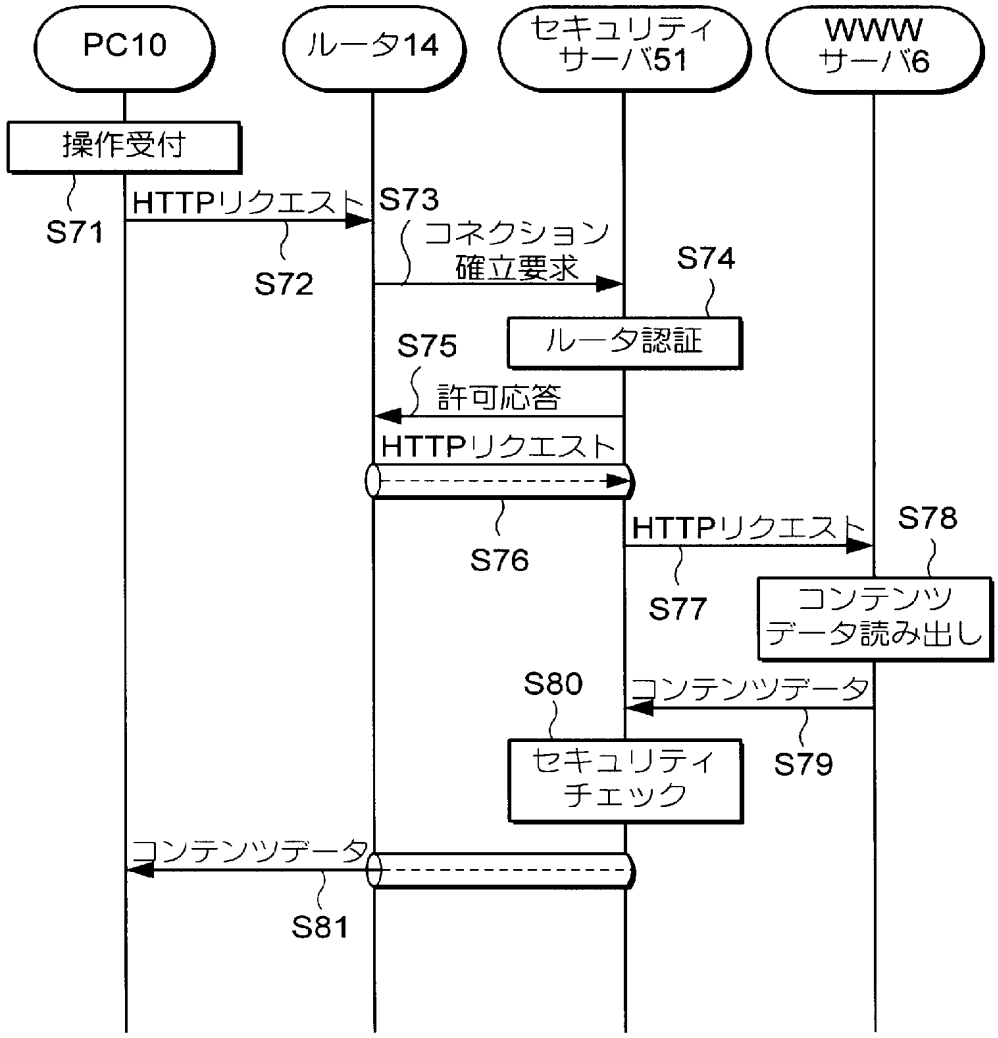
【図１８】


スタート
S101
パケットを受信？
No
Yes
S102
チェック対象プロトコルか？
No
Yes
S103
送信元がセキュリティサーバ51か？
Yes
No
S104
セキュリティサーバ51と通信コネクションを確立しているか？
No
S105
通信コネクション確立処理
Yes
IPカプセル化
S106
送　信
S107

【図１９】


PC10
ルータ14
セキュリティ
サーバ51
SMTP
サーバ33
操作受付
S51
S52
接続要求
S53
コネクション
確立要求
S54
ルータ認証
S55
許可応答
S56
接続要求
許可応答
S57
メールデータ
S58
S59
セキュリティ
チェック
S60
メールデータ
S61
受信確認
切断要求
S62

【図２０】


PC10
ルータ14
セキュリティ
サーバ51
WWW
サーバ6
操作受付
S71
HTTPリクエスト
S72
S73
コネクション
確立要求
S74
ルータ認証
S75
許可応答
HTTPリクエスト
S76
HTTPリクエスト
S77
S78
コンテンツ
データ読み出し
S80
コンテンツデータ
S79
セキュリティ
チェック
コンテンツデータ
S81

【書類名】　　要約書

【要約】

【課題】　インターネット等のコンピュータネットワークにおいて、コンピュータウィルスやジャンクメール等の様々な不正行為による被害を防止する。

【解決手段】　ルータ１４は、情報通信装置１０～１３から受信したデータをセンタ５のセキュリティサーバ５１に転送する。センタ５では、受信したデータに対してコンピュータウィルスの有無等をチェックし、チェック後のデータをそのデータの宛先へ送信する。

【選択図】　　図１

【書類名】手続補正書

【提出日】平成14年 2月27日

【あて先】特許庁長官　殿

【事件の表示】

【出願番号】特願2001-165580

【補正をする者】

【識別番号】397011166

【氏名又は名称】トレンドマイクロ株式会社

【代理人】

【識別番号】100098084

【弁理士】

【氏名又は名称】川▲崎▼　研二

【電話番号】03-3242-5481

【手続補正　1】

【補正対象書類名】特許願

【補正対象項目名】発明者

【補正方法】変更

【補正の内容】

【発明者】

【住所又は居所】アール．オー．シー，台湾，台北，チュン　フォア，エス．アールディー．エスイーシー．２，３１９，９階　トレンドマイクロインコーポレイテッド内

【氏名】リー，フランク

【発明者】

【住所又は居所】アメリカ合衆国，９５１２９，カリフォルニア，サンノゼ，ダートムア　ウェイ，６５４３

【氏名】リャン，ジェレミー　ジー

【発明者】

【住所又は居所】アメリカ合衆国，９１１０７，カリフォルニア，パサデナ，

エルカンポ　ドライブ，９６５

【氏名】チェン，エバ

【発明者】

【住所又は居所】アール．オー．シー，台湾，台北，１０４，　ジャンシャン　チュウ，ジャングウオ　エヌ　ロード，セクション１，レーン１２４，ナンバー３，５階

【氏名】リン，イジン

【提出物件の目録】

【物件名】宣誓書　1

【物件名】理由書　1

宣　誓　書

平成１４年２月12日

発明者

住所　アール．オー．シー，台湾，台北，チュン　フォア，エス．
アールディー．エスイーシー．２，３１９，９階
トレンドマイクロ　インコーポレイテッド
氏名　リー，フランク　Frank Lee

住所　アメリカ合衆国，９５１２９，カリフォルニア，サンノゼ，
ダートムア　ウェイ，６５４３
氏名　リャン，ジェレミー　ジー　Jeremy Liang

住所　アメリカ合衆国，９１１０７，カリフォルニア，パサデナ，
エルカンポ　ドライブ，９６５
氏名　チェン，エバ　Eva Chen

住所　アール．オー．シー，台湾，台北，１０４，
ジャンシャン　チュウ，ジャングウオ　エヌ　ロード，
セクション１，レーン１２４，ナンバー３，５階
氏名　リン，イジン　Yi Jin Lin

下記発明は、私共４名の共同発明であることに相違ありません。

記

１．出願番号
特願２００１－１６５５８０

２．発明の名称
データ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体

(B)20200390128

理　　由　　書

１．事件の表示

特願２００１－１６５５８０

２．発明の名称

データ通信方法、データ通信システム、データ中継装置、サーバ、プログラム及び記録媒体

本件は、発明者４名で出願すべきところ、発明者「リャン，ジェレミー　ジー」「チェン，エバ」「リン，イジン」を記載し忘れて出願してしまいました。

この誤記に至ったのは、代理人の不注意によるものであります。つきましては、上記発明者を追加致したく、必要書類を添えて提出致しますので、手続き方、宜しくお願い申し上げます。

以　上

平成１４年２月２７日

出願人代理人

弁理士　川崎　研二

出願人履歴

３９７０１１１６６

19980603

住所変更

東京都渋谷区代々木２丁目２番１号　小田急サザンタワー１０階

トレンドマイクロ株式会社

３９７０１１１６６

20031126

住所変更

東京都渋谷区代々木２－１－１　新宿マインズタワー

トレンドマイクロ株式会社